

Information complexity of the AND function in the two-party, and multiparty settings

Yuval Filmus¹, Hamed Hatami^{*2}, Yaqiao Li³, and Suzin You⁴

¹ Technion — Israel Institute of Technology, yuvalfi@cs.technion.ac.il

² McGill University, hatami@cs.mcgill.ca

³ McGill University, yaqiao.li@mail.mcgill.ca

⁴ McGill University, suzinyou.sy@gmail.com

Abstract. In a recent breakthrough paper [M. Braverman, A. Garg, D. Pankratov, and O. Weinstein, From information to exact communication, STOC’13 Proceedings of the 2013 ACM Symposium on Theory of Computing, ACM, New York, 2013, pp. 151–160.] Braverman *et al.* developed a local characterization for the zero-error information complexity in the two party model, and used it to compute the exact internal and external information complexity of the 2-bit AND function.

In this article, we extend their result to the multiparty number-in-hand model by proving that the generalization of their protocol has optimal internal and external information cost for certain distributions. Our proof has new components, and in particular it fixes some minor gaps in the proof of Braverman *et al.*

1 Introduction

Although communication complexity has since its birth been witnessing steady and rapid progress, it was not until recently that a focus on an information-theoretic approach resulted in new and deeper understanding of some of the classical problems in the area. This gave birth to a new area of complexity theory called *information complexity*. Recall that communication complexity is concerned with minimizing the amount of communication required for players who wish to evaluate a function that depends on their private inputs. Information complexity, on the other hand, is concerned with the amount of information that the communicated bits reveal about the inputs of the players to each other, or to an external observer.

One of the important achievements of information complexity is the recent result of [BGPW13] that determines the exact asymptotics of the randomized communication complexity of one of the oldest and most studied problems in communication complexity, set disjointness:

$$\lim_{\varepsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{R_{\varepsilon}(\text{DISJ}_n)}{n} \approx 0.4827. \quad (1)$$

^{*}Supported by an NSERC grant.

Here $R_\varepsilon(\cdot)$ denotes the randomized communication complexity with an error of at most ε on every input, and DISJ_n denotes the set disjointness problem. In this problem, Alice and Bob each receive a subset of $\{1, \dots, n\}$, and their goal is to determine whether their sets are disjoint or not. Prior to the discovery of these information-theoretic techniques, proving the lower bound $R_\varepsilon(\text{DISJ}_n) = \Omega(n)$ had already been a challenging problem, and even Razborov’s [Raz92] short proof of that fact is intricate and sophisticated.

Note that the set disjointness function is nothing but an OR of AND functions. More precisely, for $i = 1, \dots, n$, if x_i is the Boolean variable which represents whether i belongs to Alice’s set or not, and y_i is the corresponding variable for Bob, then $\bigvee_{i=1}^n (x_i \wedge y_i)$ is true if and only if Alice’s input intersects Bob’s input. Braverman *et al.* [BGPW13] exploited this fact to prove (1). Roughly speaking, they first determined the exact information cost of the 2-bit AND function for any underlying distribution μ on the set of inputs $\{0, 1\} \times \{0, 1\}$, and then used the fact that amortized communication equals information cost [BR14] to relate this to the communication complexity of the set disjointness problem. The constant 0.4827 in (1) is indeed the maximum of the information complexity of the 2-bit AND function over all measures μ that assign a zero mass to $(1, 1) \in \{0, 1\} \times \{0, 1\}$. That is

$$\max_{\mu: \mu(11)=0} \text{IC}_\mu(\text{AND}) \approx 0.4827,$$

where $\text{IC}_\mu(\text{AND})$ denotes the information cost of the 2-bit AND function with respect to the distribution μ with no error (See Definition 1 below). These results show the importance of knowing the exact information complexity of simple functions such as the AND function.

Although obtaining the asymptotics of $R_\varepsilon(\text{DISJ}_n)$ from the information complexity of the AND function is not straightforward and a formal proof requires overcoming some technical difficulties, the bulk of [BGPW13] is dedicated to computing the exact information complexity of the 2-bit AND function. This rather simple-looking problem had been studied previously by Ma and Ishwar [MI11, MI13], and some of the key ideas of [BGPW13] originate from their work. In [BGPW13] Braverman *et al* introduced a protocol to solve the AND function, and proved that it has optimal internal and external information cost. Interestingly this protocol is not a conventional communication protocol as it has access to a continuous clock, and the players are allowed to “buzz” at randomly chosen times. However, one can approximate it by conventional communication protocols through dividing the time into finitely many discrete units. Indeed, it is known [BGPW13] that no protocol with a bounded number of rounds can have optimal information cost for the AND function, and hence the infinite number of rounds, implicit in the continuous clock, is essential. We shall refer to this protocol as the *buzzers* protocol.

1.1 Our contributions

Fixing the argument of [BGPW13]: In order to show that the *buzzers* protocol has optimal information cost, inspired by the work of Ma and Ish-

war [MI11, MI13], Braverman *et al* came up with a local concavity condition, and showed that if a protocol satisfies this condition, then it has optimal information cost. This condition, roughly speaking, says that it suffices to verify that one does not gain any advantage over the conjectured optimal protocol if one of the players starts by sending a bit B . In the original paper [BGPW13], it is claimed that it suffices to verify this condition only for signals B that reveal arbitrarily small information about the inputs. As we shall see, however, this is not true, and one can easily construct counter-examples to this statement.

In Theorem 5 we prove a variant of the local concavity condition that allows one to consider only signals B with small information leakage, and then apply it to fix the argument in [BGPW13]. We have been informed through private communication that Braverman *et al* have also independently fixed the argument in [BGPW13].

Extension of [BGPW13] to the multi-party setting: We then apply Theorem 5 to extend the result of [BGPW13] to the multiparty number-in-hand model by defining a generalization of the *buzzers* protocol, and then prove in Theorem 6 that it has optimal internal and external information cost when the underlying distribution satisfies the following assumption:

Assumption 1. *The support of μ is a subset of $\{0, 1, e_1, \dots, e_k\}$, where e_i is the usual i^{th} basis vector $(0, \dots, 0, 1, 0, \dots, 0)$.*

Note that in the two-party setting, every distribution satisfies this assumption and thus our results are complete generalizations of the results of [BGPW13] in the two party setting. The distribution in Assumption 1 arise naturally in the study of the set disjointness problem, and as a result they have been considered previously in [Gro09].

This extension is not straightforward since in [BGPW13], a large part of the calculations for verifying the local concavity conditions are carried out by the software Mathematica. However, in the number-in-hand model, having an arbitrary number of players, one cannot simply rely on a computer program for those calculations. Instead, first we had to analyze and understand what happens at different stages of the protocol, and once we reduced the problem to sufficiently simple equations (with a constant number of variables), then we used a computer program to verify them. We believe our proof provides some new insights even for the two-party setting.

2 Preliminaries

2.1 Notation

We typically denote the random variables by capital letters (e.g A, B, C, X, Y, Π). For the sake of brevity, we shall write $A_1 \dots A_n$ to denote the random variable (A_1, \dots, A_n) and *not* the product of the A_i 's. We use $[n]$ to denote the set $\{1, \dots, n\}$, and $\text{supp}(\mu)$ to denote the support of a measure μ . We denote the statistical distance (a.k.a. total variation distance) of two measures μ and ν on the sample space Ω by $|\mu - \nu| := \frac{1}{2} \sum_{a \in \Omega} |\mu(a) - \nu(a)|$.

For every $\varepsilon \in [0, 1]$, $H(\varepsilon) = -\varepsilon \log \varepsilon - (1 - \varepsilon) \log(1 - \varepsilon)$ denotes the binary entropy, where here and throughout the paper $\log(\cdot)$ is in base 2, and $0 \log 0 = 0$.

Recall $D(\mu||\nu)$ means the divergence (a.k.a. relative entropy, or Kullback Leibler distance) between two distributions μ and ν . Let X and Y be two random variables, the standard notation $I(X, Y)$ means the mutual information between X and Y , sometimes we use the notation $D(X||Y)$ to denote the divergence between the distributions of X and Y . For definitions and basic facts regarding divergence and mutual information, see [CT12].

2.2 Communication complexity

The notion of two-party communication complexity was introduced by Yao [Yao79] in 1979. In this model there are two players (with unlimited computational power), often called Alice and Bob, who wish to collaboratively compute a given function $f: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$. Alice receives an input $x \in \mathcal{X}$ and Bob receives $y \in \mathcal{Y}$. Neither of them knows the other player's input, and they wish to communicate in accordance with an agreed-upon protocol π to compute $f(x, y)$. The protocol π specifies as a function of (only) the transmitted bits whether the communication is over, and if not, who sends the next bit. Furthermore π specifies what the next bit must be as a function of the transmitted bits, and the input of the player who sends the bit. The *cost* of the protocol is the total number of bits transmitted on the worst case input. The *transcript* Π of a protocol π is the list of all the transmitted bits during the execution of the protocol.

In the randomized communication model, the players might have access to a shared random string (*public randomness*), and their own private random strings (*private randomness*). These random strings are independent, but they can have any desired distributions individually. In the randomized model the transcript also includes the public random string in addition to the transmitted bits. Similar to the case of deterministic protocols, the *cost* is the total number of bits transmitted on the worst case input and random strings. The *average cost* of the protocol is the expected number of bits transmitted on the worst case input.

For a function $f: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ and a parameter $\varepsilon > 0$, we denote by $R_\varepsilon(f)$ the cost of the best randomized protocol for computing f with probability of error at most ε on *every* input.

2.3 Information complexity

The setting is the same as in communication complexity, where Alice and Bob (having infinite computational power) wish to mutually compute a function $f: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$. To be able to measure information, we also need to assume that there is a prior distribution μ on $\mathcal{X} \times \mathcal{Y}$.

For the purpose of communication complexity, once we allow public randomness, it makes no difference whether we permit the players to have private random strings or not. This is because the private random strings can be simulated by parts of the public random string. On the other hand, for information

complexity, it is crucial to permit private randomness, and once we allow private randomness, public randomness becomes inessential. Indeed, one of the players can use her private randomness to generate the public random string, and then transmit it to the other player. Although this might have very large communication cost, it has no information cost, as it does not reveal any information about the players' input.

Probably the most natural way to define the information cost of a protocol is to consider the amount of information that is revealed about the inputs X and Y to an external observer who sees the transmitted bits and the public randomness. This is known as the *external information cost* and is formally defined as the mutual information between XY and the transcript of the protocol (recall that the transcript Π_{XY} contains the public random string R). While this notion is interesting and useful, it turns out there is another way of defining information cost that has some very useful properties. This is called the *internal information cost* or just the *information cost* for short, and is equal to the amount of information that Alice and Bob learn about each other's input from the communication. Note that Bob knows Y , the public randomness R and his own private randomness R_B , and thus what he learns about X from the communication can be measured by $I(X; \Pi | Y R R_B)$. Similarly, what Alice learns about Y from the communication can be measured by $I(Y; \Pi | X R R_A)$ where R_A is Alice's private random string. It is not difficult to see [BBCR10] that conditioning on the public and private randomness does not affect these quantities. In other words $I(X; \Pi | Y R R_B) = I(X; \Pi | Y)$ and $I(Y; \Pi | X R R_A) = I(Y; \Pi | X)$. We summarize these in the following definition.

Definition 1. *The external information cost and the internal information cost of a protocol π with respect to a distribution μ on inputs from $\mathcal{X} \times \mathcal{Y}$ are defined as*

$$\text{IC}_\mu^{\text{ext}}(\pi) = I(\Pi; XY),$$

and

$$\text{IC}_\mu(\pi) = I(\Pi; X|Y) + I(\Pi; Y|X),$$

respectively, where $\Pi = \Pi_{XY}$ is the transcript of the protocol when it is executed on the inputs XY .

We will be interested in certain *communication tasks*. Let $[f, \varepsilon]$ denote the task of computing the value of $f(x, y)$ correctly with probability at least $1 - \varepsilon$ for every (x, y) . Thus a protocol π performs this task if

$$\Pr[\pi(x, y) \neq f(x, y)] \leq \varepsilon, \quad \forall (x, y) \in \mathcal{X} \times \mathcal{Y}. \quad (2)$$

Given another distribution ν on $\mathcal{X} \times \mathcal{Y}$, let $[f, \nu, \varepsilon]$ denote the task of computing the value of $f(x, y)$ correctly with probability at least $1 - \varepsilon$ if the input (x, y) is sampled from the distribution ν . A protocol π performs this task if

$$\Pr_{(x, y) \sim \nu} [\pi(x, y) \neq f(x, y)] \leq \varepsilon. \quad (3)$$

Note that a protocol π performs $[f, 0]$ if it computes f correctly on *every* input while performing $[f, \nu, 0]$ means computing f correctly on the inputs that belong to the support of ν .

The *information complexity* of a communication task T with respect to a measure μ is defined as

$$\text{IC}_\mu(T) = \inf_{\pi: \pi \text{ performs } T} \text{IC}_\mu(\pi). \quad (4)$$

It is essential here that we use infimum rather than minimum as there are tasks for which there is no protocol that achieves $\text{IC}_\mu(T)$ while there is a sequence of protocols whose information cost converges to $\text{IC}_\mu(T)$. The *external information complexity* of a communication task T is defined similarly. We will abbreviate $\text{IC}_\mu(f, \varepsilon) = \text{IC}_\mu([f, \varepsilon])$, $\text{IC}_\mu(f, \nu, \varepsilon) = \text{IC}_\mu([f, \nu, \varepsilon])$, etc. It is important to note that when μ does not have full support, $\text{IC}_\mu(f, \mu, 0)$ can be strictly smaller than $\text{IC}_\mu(f, 0)$. We sometimes also abbreviate $\text{IC}_\mu(f) = \text{IC}_\mu(f, 0)$.

Remark 1 (A warning regarding our notation). In the literature of information complexity it is common to use “ $\text{IC}_\mu(f, \varepsilon)$ ” to denote the distributional error case, i.e. what we denote by $\text{IC}_\mu(f, \mu, \varepsilon)$. Unfortunately this has become the source of some confusions in the past, as sometimes “ $\text{IC}_\mu(f, \varepsilon)$ ” is used to denote both of the distributional error $[f, \mu, \varepsilon]$ and the point-wise error $[f, \varepsilon]$. To avoid ambiguity we distinguish the two cases by using the different notations $\text{IC}_\mu(f, \mu, \varepsilon)$ and $\text{IC}_\mu(f, \varepsilon)$.

2.4 The continuity of information complexity

The information complexities $\text{IC}_\mu(f, \varepsilon)$ and $\text{IC}_\mu(f, \nu, \varepsilon)$ are both continuous with respect to ε . The following simple lemma from [Bra15] proves the continuity for $\varepsilon \in (0, 1]$. The continuity at 0 is more complicated and is proven in [BGPW13].

Lemma 1. [Bra15] *For every $f: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, $\varepsilon_2 > \varepsilon_1 > 0$ and measures μ, ν on $\mathcal{X} \times \mathcal{Y}$, we have*

$$\text{IC}_\mu(f, \nu, \varepsilon_1) - \text{IC}_\mu(f, \nu, \varepsilon_2) \leq (1 - \varepsilon_1/\varepsilon_2) \log |\mathcal{X} \times \mathcal{Y}|, \quad (5)$$

Proof. Let $f: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, and consider a protocol π with information cost I , and error $\varepsilon_2 > 0$. Set $\delta = 1 - \varepsilon_1/\varepsilon_2$, and let τ be the following protocol

- With probability $1 - \delta$ run π .
- With probability δ Alice and Bob exchange their inputs and compute $f(x, y)$.

The theorem follows as the new protocol has error at most $(1 - \delta)\varepsilon_2 = \varepsilon_1$, and information cost at most $I + \delta \log |\mathcal{X} \times \mathcal{Y}|$. \square

Remark 2. The same proof implies $\text{IC}_\mu(f, \varepsilon_1) - \text{IC}_\mu(f, \varepsilon_2) \leq (1 - \varepsilon_1/\varepsilon_2) \log |\mathcal{X} \times \mathcal{Y}|$.

Note that $\text{IC}_\mu(f, \mu, 0)$ is not always continuous with respect to μ . For example, let

$$\mu_\varepsilon = \begin{pmatrix} \frac{1-\varepsilon}{3} & \frac{1-\varepsilon}{3} \\ \frac{1-\varepsilon}{3} & \varepsilon \end{pmatrix}, \quad \mu = \lim_{\varepsilon \rightarrow 0} \mu_\varepsilon = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 \end{pmatrix}. \quad (6)$$

Now for the 2-bit AND function, we have $\text{IC}_\mu(\text{AND}, \mu, 0) = 0$, while $\text{IC}_{\mu_\varepsilon}(\text{AND}, \mu_\varepsilon, 0) = \text{IC}_{\mu_\varepsilon}(\text{AND})$ as μ_ε has full support. Thus

$$\lim_{\varepsilon \rightarrow 0} \text{IC}_{\mu_\varepsilon}(\text{AND}, \mu_\varepsilon, 0) = \lim_{\varepsilon \rightarrow 0} \text{IC}_{\mu_\varepsilon}(\text{AND}) = \text{IC}_\mu(\text{AND}),$$

which is known to be bounded away from 0. The same example also shows that $\text{IC}_\mu(f, \mu, \varepsilon)$ is not always continuous with respect to ε at $\varepsilon = 0$ if μ depends on ε . In fact, $\text{IC}_{\mu_\varepsilon}(\text{AND}, \mu_\varepsilon, \varepsilon) = 0$ while $\text{IC}_{\mu_\varepsilon}(\text{AND}, \mu_\varepsilon, 0) = \text{IC}_{\mu_\varepsilon}(\text{AND})$ for all $\varepsilon > 0$, hence when $\varepsilon > 0$ is sufficiently small we find $\text{IC}_{\mu_\varepsilon}(\text{AND}, \mu_\varepsilon, 0)$ is close to $\text{IC}_\mu(\text{AND})$ which is bounded away from 0.

However it turns out that $\text{IC}_\mu(f, \nu, \varepsilon)$ is continuous with respect to μ for all $\varepsilon \geq 0$ when ν is fixed. This follows from the fact, established in [BGPW16, Lemma 4.4], that for every protocol π and every two measures μ_1 and μ_2 with $|\mu_1 - \mu_2| \leq \delta$ (the distribution metric is statistical distance), we have

$$|\text{IC}_{\mu_1}(\pi) - \text{IC}_{\mu_2}(\pi)| \leq 2 \log(|\mathcal{X} \times \mathcal{Y}|) \delta + 2H(2\delta). \quad (7)$$

Consequently

$$|\text{IC}_{\mu_1}(f, \nu, \varepsilon) - \text{IC}_{\mu_2}(f, \nu, \varepsilon)| \leq 2 \log(|\mathcal{X} \times \mathcal{Y}|) \delta + 2H(2\delta),$$

as $\text{IC}_{\mu_1}(f, \nu, \varepsilon) = \inf_\pi \text{IC}_{\mu_1}(\pi)$ and $\text{IC}_{\mu_2}(f, \nu, \varepsilon) = \inf_\pi \text{IC}_{\mu_2}(\pi)$ where both infimums are over all protocols π that computes $[f, \nu, \varepsilon]$. In particular, by taking $\varepsilon = 0$ and ν to be a measure with full support, we get the following theorem.

Theorem 1 ([BGPW16, Lemma 4.4]). *$\text{IC}_\mu(f)$ is uniformly continuous with respect to μ .*

Finally, note that if $|\nu_1 - \nu_2| \leq \delta \leq \varepsilon$, then

$$\text{IC}_\mu(f, \nu_1, \varepsilon + \delta) \leq \text{IC}_\mu(f, \nu_2, \varepsilon) \leq \text{IC}_\mu(f, \nu_1, \varepsilon - \delta). \quad (8)$$

This proves the continuity with respect to ν when $\varepsilon > 0$. The following theorem summarizes the continuity of $\text{IC}_\mu(f, \nu, \varepsilon)$ with respect to its parameters.

Theorem 2 (Uniform continuity with error). *Consider $\delta > 0$. For each $f: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, real numbers $\varepsilon_2 \geq \varepsilon_1 \geq \delta$, and measures $\mu_1, \mu_2, \nu_1, \nu_2$ on $\mathcal{X} \times \mathcal{Y}$ with $|\mu_1 - \mu_2| \leq \delta$ and $|\nu_1 - \nu_2| \leq \delta$, we have*

$$|\text{IC}_{\mu_1}(f, \nu_1, \varepsilon_1) - \text{IC}_{\mu_2}(f, \nu_2, \varepsilon_2)| \leq \left(1 - \frac{\varepsilon_1}{\varepsilon_2} + \frac{4\delta}{\varepsilon_1}\right) \log |\mathcal{X} \times \mathcal{Y}| + 2H(2\delta).$$

Proof. By (5), we have

$$|\text{IC}_{\mu_2}(f, \nu_2, \varepsilon_2) - \text{IC}_{\mu_2}(f, \nu_2, \varepsilon_1)| \leq (1 - \frac{\varepsilon_1}{\varepsilon_2}) \log(|\mathcal{X} \times \mathcal{Y}|).$$

By (8) and (5), we have

$$|\text{IC}_{\mu_2}(f, \nu_2, \varepsilon_1) - \text{IC}_{\mu_2}(f, \nu_1, \varepsilon_1)| \leq (1 - \frac{\varepsilon_1 - \delta}{\varepsilon_1 + \delta}) \log(|\mathcal{X} \times \mathcal{Y}|) \leq \frac{2\delta}{\varepsilon_1} \log(|\mathcal{X} \times \mathcal{Y}|).$$

By (7), we have

$$|\text{IC}_{\mu_2}(f, \nu_1, \varepsilon_1) - \text{IC}_{\mu_1}(f, \nu_1, \varepsilon_1)| \leq 2 \log(|\mathcal{X} \times \mathcal{Y}|) \delta + 2H(2\delta).$$

These three inequalities imply the theorem. \square

2.5 The multiparty number-in-hand model

The number-in-hand model is the most straightforward generalization of Yao's two-party model to the settings where more than two players are present. In this model there are k players who wish to collaboratively compute a function $f: \mathcal{X}_1 \times \dots \times \mathcal{X}_k \rightarrow \mathcal{Z}$. The communication is in the shared blackboard model, which means that all the communicated bits are visible to all the players. Let μ be a probability distribution on $\mathcal{X}_1 \times \dots \times \mathcal{X}_k$, and let $X = (X_1, \dots, X_k)$ be sampled from $\mathcal{X}_1 \times \dots \times \mathcal{X}_k$ according to μ . Definition 1 generalizes in a straightforward manner to

$$\text{IC}_{\mu}^{\text{ext}}(\pi) = I(\Pi; X),$$

and

$$\text{IC}_{\mu}(\pi) = \sum_{i=1}^k I(\Pi; X_{-i} | X_i),$$

where $X_{-i} := (X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_k)$. Note also that $I(\Pi; X | X_i) = I(\Pi; X_{-i} | X_i)$, and thus we have

$$\text{IC}_{\mu}(\pi) = \sum_{i=1}^k I(\Pi; X | X_i).$$

The notations $\text{IC}_{\mu}(f)$, $\text{IC}_{\mu}(f, \varepsilon)$, and $\text{IC}_{\mu}(f, \nu, \varepsilon)$, and the continuity results in Section 2.4 also generalize in a straightforward manner to this setting.

3 The local characterization of the optimal information cost

We start by some definitions. Let B be a random bit sent by one of the players, and let $\mu_0 = \mu|_{B=0}$ and $\mu_1 = \mu|_{B=1}$, or in other words

$$\mu_b(xy) := \Pr[XY = xy | B = b],$$

for $b = 0, 1$. Denote $\Pr[\cdot | xy] := \Pr[\cdot | XY = xy]$.

Definition 2. Let μ be a distribution and B be a signal sent by one of the players.

- B is called unbiased with respect to μ if $\Pr[B = 0] = \Pr[B = 1] = \frac{1}{2}$.
- B is called non-crossing if $\mu(xy) < \mu(x'y')$ implies that $\mu_b(xy) \leq \mu_b(x'y')$ for $b = 0, 1$.
- B is called ε -weak if $|\Pr[B = 0|xy] - \Pr[B = 1|xy]| \leq \varepsilon$ for every input xy .

A protocol is said to be in normal form with respect to μ if all its signals are unbiased and non-crossing with respect to μ .

Let $\Delta(\mathcal{X} \times \mathcal{Y})$ denote the set of distributions on $\mathcal{X} \times \mathcal{Y}$. A measure $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ is said to be *internal-trivial* (resp. *external-trivial*) for f if $\text{IC}_\mu(f) = 0$ (resp. $\text{IC}_\mu^{\text{ext}}(f) = 0$). These measures are characterized in [DFHL16].

3.1 The Local Characterization

Suppose that after a random bit B is sent, if $B = 0$, the players continue by running a protocol that is (almost) optimal for μ_0 , and if $B = 1$, they run a protocol that is (almost) optimal for μ_1 . Note that the amount of information that B reveals about the inputs to an external observer is $I(B; XY)$. This shows

$$\text{IC}_\mu^{\text{ext}}(f) \leq I(B; XY) + \mathbb{E}_B[\text{IC}_{\mu_B}^{\text{ext}}(f)], \quad (9)$$

and similarly

$$\text{IC}_\mu(f) \leq I(B; X|Y) + I(B; Y|X) + \mathbb{E}_B[\text{IC}_{\mu_B}(f)]. \quad (10)$$

In [BGPW13] it is shown that these inequalities essentially characterize $\text{IC}_\mu^{\text{ext}}(f, \mu, 0)$ and $\text{IC}_\mu(f, \mu, 0)$. Denote $\text{I}_B^{\text{ext}} := I(B; XY)$, and $\text{I}_B := I(B; X|Y) + I(B; Y|X)$.

Theorem 3 ([BGPW13]). Suppose that $C: \Delta(\mathcal{X} \times \mathcal{Y}) \rightarrow [0, \log(|\mathcal{X} \times \mathcal{Y}|)]$ satisfies

- (i) $C(\mu) = 0$ for every measure μ such that $\text{IC}_\mu(f, \mu, 0) = 0$, and
- (ii) for every signal B that can be sent by one of the players

$$C(\mu) \leq \text{I}_B + \mathbb{E}_B[C(\mu_B)].$$

Then $C(\mu) \leq \text{IC}_\mu(f, \mu, 0)$. Similarly if $\text{IC}_\mu(f, \mu, 0)$ is replaced by $\text{IC}_\mu^{\text{ext}}(f, \mu, 0)$, and I_B is replaced by I_B^{ext} , then $C(\mu) \leq \text{IC}_\mu^{\text{ext}}(f, \mu, 0)$. Furthermore, in both of the external and the internal cases, it suffices to verify (ii) only for non-crossing unbiased signals B .

In light of Theorem 3, in order to determine the values of $\text{IC}_\mu(f, \mu, 0)$, one has to first prove an upper bound by constructing a protocol (or a sequence of protocols) for every measure μ . Then it suffices to verify that the bound satisfies the conditions of Theorem 3.

In [BGPW13], $\text{IC}_\mu(\text{AND}_2)$ is determined using Theorem 3. However, the proof presented in [BGPW13] contains some gaps. One error is the claim that it suffices to verify (ii) for sufficiently weak signals. While it is not difficult to see that indeed it suffices to verify (ii) for signals B which are ε -weak for an absolute constant $\varepsilon > 0$, in [BGPW13] the condition (ii) is only verified for ε that is smaller than a function of μ . This is not sufficient, and one can easily construct a counter-example by allowing the signal B to become increasingly weaker as μ moves closer to the boundary (by boundary we mean the set of measures μ that satisfy Theorem 3 (i)). Indeed, for example, set $C(\mu) = K$ for a very large constant K if μ does not satisfy Theorem 3 (i), and otherwise set $C(\mu) = 0$. Obviously (ii) holds if μ is on the boundary. On the other hand, if μ is not on the boundary, then by taking B to be sufficiently weak as a function of μ , we can guarantee that μ_0 and μ_1 are not on the boundary either, and thus (ii) holds in this case as well. However, taking K to be sufficiently large violates the desired conclusion that $C(\mu) \leq \text{IC}_\mu(f, \mu, 0)$.

To fix these errors, we start by observing that a straightforward adaptation of the proof of Theorem 3 yields an identical characterization of $\text{IC}_\mu(f)$, however, with a different boundary condition.

Theorem 4. *Suppose that $C: \Delta(\mathcal{X} \times \mathcal{Y}) \rightarrow [0, \log(|\mathcal{X} \times \mathcal{Y}|)]$ satisfies*

- (i) $C(\mu) = 0$ for every measure μ such that $\text{IC}_\mu(f) = 0$, and
- (ii) for every signal B that can be sent by one of the players

$$C(\mu) \leq I_B + \mathbb{E}_B[C(\mu_B)].$$

Then $C(\mu) \leq \text{IC}_\mu(f)$. Similarly, if we replace $\text{IC}_\mu(f)$ by $\text{IC}_\mu^{\text{ext}}(f)$, and I_B by I_B^{ext} , then $C(\mu) \leq \text{IC}_\mu^{\text{ext}}(f)$. Furthermore, in both cases, it suffices to verify (ii) only for non-crossing unbiased signals B .

Proof. We only prove the internal case as the external case is similar. Let π be a c -bit protocol in normal form and Π be its transcript. For every possible transcript t , let $\mu_t := \mu|_{\Pi=t}$. Condition (ii) says that for every 1-bit protocol π ,

$$C(\mu) \leq \text{IC}_\mu(\pi) + \mathbb{E}_{t \sim \Pi}[C(\mu_t)]. \quad (11)$$

By a simple induction (see [BGPW13, Lemma 5.6]) this implies that (11) holds for every c -bit protocol π in a normal form where $c < \infty$.

Now consider an arbitrary protocol τ that computes $[f, 0]$. Lemma 4 below shows that one can simulate τ with a protocol π that is in normal form and terminates with probability 1. Note that π also computes $[f, 0]$ and by Proposition 1 we have $\text{IC}_\mu(\tau) = \text{IC}_\mu(\pi)$.

Consider a large integer c , and let π_c be the protocol that is obtained by truncating π after c bits of communication, clearly $\text{IC}_\mu(\pi_c) \leq \text{IC}_\mu(\pi)$ as π_c is a truncation of π . Let G_c denote the set of leaves of π_c in which the protocol is forced to terminate, and had we run π instead, the communication would have

continued. Let Π_c denote the transcript of π_c . For any given $\delta > 0$, one can guarantee that for every xy ,

$$\Pr[\Pi_c(xy) \in G_c] < \delta$$

by choosing c to be sufficiently large. As π computes $[f, 0]$, for every leaf t in π_c such that $t \notin G_c$, μ_t is an internal-trivial distribution, hence Condition (i) is satisfied on μ_t implying $C(\mu_t) = 0$. Therefore (11) shows

$$C(\mu) \leq \text{IC}_\mu(\pi_c) + \delta \log(|\mathcal{X} \times \mathcal{Y}|) \leq \text{IC}_\mu(\pi) + \delta \log(|\mathcal{X} \times \mathcal{Y}|) = \text{IC}_\mu(\tau) + \delta \log(|\mathcal{X} \times \mathcal{Y}|).$$

Letting $\delta \rightarrow 0$ one obtains the desired bound. \square

We use the uniform continuity of $\text{IC}_\mu(f)$ with respect to μ to prove that it suffices to verify Theorem 4 (ii) for signals B that are weaker than quantities that can depend on μ . This as we shall see suffices to fix the proof of [BGPW13].

Theorem 5 (Main Theorem 1). *Let $w: (0, 1] \rightarrow (0, 1]$ be a non-decreasing function, $\Omega \subseteq \Delta(\mathcal{X} \times \mathcal{Y})$ be a subset of measures containing the internal trivial distributions for function f . Let $\delta(\mu)$ denote the distance of μ from Ω . Suppose that $C: \Delta(\mathcal{X} \times \mathcal{Y}) \rightarrow [0, \log(|\mathcal{X} \times \mathcal{Y}|)]$ satisfies*

- (i) $C(\mu)$ is uniformly continuous with respect to μ ;
- (ii) $C(\mu) = \text{IC}_\mu(f)$ if $\delta(\mu) = 0$, and
- (iii) for every non-crossing unbiased $w(\delta(\mu))$ -weak signal B that can be sent by one of the players,

$$C(\mu) \leq I_B + \mathbb{E}_B[C(\mu_B)]. \quad (12)$$

Then $C(\mu) \leq \text{IC}_\mu(f)$. Similarly, if we replace Ω by a subset containing the external trivial distributions for function f , in Condition (ii) replace $\text{IC}_\mu(f)$ by $\text{IC}_\mu^{\text{ext}}(f)$, and in Condition (iii) replace I_B by I_B^{ext} , then $C(\mu) \leq \text{IC}_\mu^{\text{ext}}(f)$.

The proof of Theorem 5 is presented in Section 4.2.

3.2 The local characterization in a different form

Information cost measures the amount of information that is revealed by communicated bits. The local concavity conditions in Section 3.1 become more natural if they are represented in terms of the amount of information that is *not* revealed. Define the *concealed information* and *external concealed information* of a protocol π with respect to μ , respectively, as

$$\text{CI}_\mu(\pi) = H(X|\Pi Y) + H(Y|\Pi X) = H(X|Y) + H(Y|X) - \text{IC}_\mu(\pi),$$

and

$$\text{CI}_\mu^{\text{ext}}(\pi) = H(XY|\Pi) = H(XY) - \text{IC}_\mu^{\text{ext}}(\pi),$$

where Π is the transcript of π .

Remark 3. In the setting of multi-party number-in-hand model, we have

$$\text{CI}_\mu(\pi) = \sum_{i=1}^k H(X|\Pi X_i) = \left(\sum_{i=1}^k H(X|X_i) \right) - \text{IC}_\mu(\pi),$$

and

$$\text{CI}_\mu^{\text{ext}}(\pi) = H(X|\Pi) = H(X) - \text{IC}_\mu^{\text{ext}}(\pi),$$

where $X = (X_1, \dots, X_k)$ is the random vector of all inputs.

By using concealed information rather than information cost, the local characterization turns into a condition about the local concavity of the function.

Lemma 2. *Inequalities (9) and (10) are respectively equivalent to*

$$\text{CI}_\mu^{\text{ext}}(f) \geq \mathbb{E}_B[\text{CI}_{\mu_B}^{\text{ext}}(f)], \quad \text{and} \quad \text{CI}_\mu(f) \geq \mathbb{E}_B[\text{CI}_{\mu_B}(f)].$$

Proof. Substituting $I(B; XY) = H(XY) - H(XY|B)$ in $\text{IC}_\mu^{\text{ext}}(f) \leq I(B; XY) + \mathbb{E}_B[\text{IC}_{\mu_B}^{\text{ext}}(f)]$ leads to

$$\text{CI}_\mu^{\text{ext}}(f) \geq H(XY|B) - \mathbb{E}_B[H(XY|B=b) - \text{CI}_{\mu_B}^{\text{ext}}(f)]$$

which simplifies to the desired $\text{CI}_\mu^{\text{ext}}(f) \geq \mathbb{E}_B[\text{CI}_{\mu_B}^{\text{ext}}(f)]$.

Similarly substituting $I(B; X|Y) + I(B; Y|X) = H(X|Y) - H(X|YB) + H(Y|X) - H(Y|XB)$ in $\text{IC}_\mu(f) \leq I(B; X|Y) + I(B; Y|X) + \mathbb{E}_B[\text{IC}_{\mu_B}(f)]$ leads to

$$\text{CI}_\mu(f) \geq H(X|YB) + H(Y|XB) - \mathbb{E}_B[H(X|YB=b) + H(Y|XB=b) - \text{IC}_{\mu_B}(f)]$$

which simplifies to $\text{CI}_\mu(f) \geq \mathbb{E}_B[\text{CI}_{\mu_B}(f)]$. \square

4 Communication protocols as random walks on $\Delta(\mathcal{X} \times \mathcal{Y})$

Consider a protocol π and a prior distribution μ on the set of inputs $\mathcal{X} \times \mathcal{Y}$. Suppose that in the first round Alice sends a random signal B to Bob. We can interpret this as a random update of the prior distribution μ to a new distribution $\mu_0 = \mu|_{B=0}$ or $\mu_1 = \mu|_{B=1}$ depending on the value of B . It is not difficult to see that $\mu_b(x, y) = p_b(x)\mu(x, y)$ for $b = 0, 1$, where $p_b(x) = \frac{\Pr[B=b|x]}{\Pr[B=b]}$. In other words, μ_b is obtained by multiplying the rows of μ by non-negative numbers. Similarly if Bob is sending a message, then μ_b is obtained by multiplying the columns of μ by the numbers $p_b(y) = \frac{\Pr[B=b|y]}{\Pr[B=b]}$. That is $\mu_b(x, y) = \mu(x, y)p_b(y)$. Therefore, we can think of a protocol as a random walk on $\Delta(\mathcal{X} \times \mathcal{Y})$ that starts at μ , and every time that a player sends a message, it moves to a new distribution. Note further that this random walk is without drift as $\mu = \mathbb{E}_B[\mu_B]$.

Let Π denote the transcript of the protocol. When the protocol terminates, the random walk stops at $\mu_\Pi := \mu|_\Pi$. Since Π itself is a random variable, μ_Π is a random variable that takes values in $\Delta(\mathcal{X} \times \mathcal{Y})$. Interestingly, both the internal and external information costs of the protocol depend only on the distribution of μ_Π (this is a distribution on the set $\Delta(\mathcal{X} \times \mathcal{Y})$, which itself is a set of distributions). To see this, note $I(X; \Pi|Y) = \mathbb{E}_{\pi \sim \Pi, y \sim Y} D(X|_{\Pi=\pi, Y=y} \| X|_{Y=y})$ and $I(XY; \Pi) = \mathbb{E}_{\pi \sim \Pi} D(XY|_{\Pi=\pi} \| XY)$, and thus both of these quantities are determined by μ and μ_Π . This immediately leads to the following observation:

Proposition 1. [BS15] *Let π and τ be two communication protocols with the same input set $\mathcal{X} \times \mathcal{Y}$ endowed with a probability measure μ . Let Π and T denote the transcripts of π and τ , respectively. If μ_Π has the same distribution as μ_T , then $\text{IC}_\mu(\pi) = \text{IC}_\mu(\tau)$ and $\text{IC}_\mu^{\text{ext}}(\pi) = \text{IC}_\mu^{\text{ext}}(\tau)$.*

Proposition 1 shows that in the context of information complexity, it does not matter how different the steps of two protocol are, and as long as they both yield the same distribution on $\Delta(\mathcal{X} \times \mathcal{Y})$, they have the same internal and external information cost. Consequently, one can directly work with this random walk (or the resulting distribution on $\Delta(\mathcal{X} \times \mathcal{Y})$) instead of working with the actual protocols. Indeed, let $\mathcal{C}_\mu^T(\Delta(\mathcal{X} \times \mathcal{Y}))$ denote the set of all probability distributions on $\Delta(\mathcal{X} \times \mathcal{Y})$ that can be obtained, starting from the distribution μ , through communication protocols that perform a given communication task T . The information cost of performing the task T is the infimum of the information costs of the distributions in $\mathcal{C}_\mu^T(\Delta(\mathcal{X} \times \mathcal{Y}))$. Although, as mentioned earlier, this infimum is not always attained, if one takes the closure of $\mathcal{C}_\mu^T(\Delta(\mathcal{X} \times \mathcal{Y}))$ (under weak convergence) then one can replace the infimum with minimum. For the 2-bit AND function, the buzzers protocol of [BGPW13] yields the distribution in the closure of $\mathcal{C}_\mu^T(\Delta(\mathcal{X} \times \mathcal{Y}))$ that achieves the minimum information cost. The buzzers protocol is not a communication protocol, but one can consider it as the limit of a sequence of communication protocols. We believe that the following is an important open problem.

Problem 1. Define a paradigm such that for every communication task T and every measure μ on an input set $\mathcal{X} \times \mathcal{Y}$, the set of distributions on $\Delta(\mathcal{X} \times \mathcal{Y})$ resulting from the protocols performing the task T in this paradigm is exactly equal to the closure of $\mathcal{C}_\mu^T(\Delta(\mathcal{X} \times \mathcal{Y}))$.

Partial progress towards resolving this problem has been made in [DF16], see also [DFHL16].

4.1 A signal simulation lemma

Here we prove a simulation lemma that will be useful in the proof of the local characterization theorems. We start by restating a splitting lemma from [BGPW13]. We use the notation $[\mu_0, \mu_1]$ for the set of all convex combinations $\alpha\mu_0 + (1 - \alpha)\mu_1$, where $\alpha \in [0, 1]$.

Lemma 3 (Splitting Lemma, [BGPW13]). Consider $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ and a signal B sent by one of the players, and let $\mu_b = \mu|_{B=b}$ for $b = 0, 1$. Consider $\rho_0, \rho_1 \in [\mu_0, \mu_1]$ and $\rho \in (\rho_0, \rho_1)$. There exists a signal B' that the same player can send starting at ρ such that $\rho_b = \rho|_{B'=b}$ for $b = 0, 1$.

Lemma 3 is proved in [BGPW13, Lemma 7.11], there is a minor error in the original statement as it is claimed that the lemma holds for $\rho \in [\rho_0, \rho_1]$ where the interval is closed.

We are now ready to prove the signal simulation lemma, which says every signal can be perfectly simulated by a non-crossing unbiased ε -weak signal sequence. This lemma generalizes [BGPW13, Lemma 5.2].

Lemma 4 (Signal Simulation). Let $\varepsilon > 0$, and consider $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ and a signal B sent by one of the players. There exists a sequence of non-crossing unbiased ε -weak random signals $\mathcal{B} = (B_1 B_2 \dots)$ that with probability 1 terminates, and furthermore $\mu|_{\mathcal{B}}$ has the same distribution as $\mu|_B$.

Proof. Let $\mu_0 = \mu|_{B=0}$ and $\mu_1 = \mu|_{B=1}$. The following protocol explains how the sequence $(B_1 B_2 \dots)$ is constructed from the signal B .

- Set $\mu_c = \mu$ and $i = 1$;
- Repeat until $\mu_c = \mu_0$ or $\mu_c = \mu_1$;
- If $\mu_c \in [\mu_0, \mu]$, then
 - Set λ to be the largest value in $[0, 1]$ satisfying
 - $\lambda \max_{xy} \frac{|\mu_c(x, y) - \mu_0(x, y)|}{\mu_c(x, y)} \leq \varepsilon$, and
 - $\lambda |\mu_0(x, y) - \mu_0(x', y') - \mu_c(x, y) + \mu_c(x', y')| \leq \mu_c(x', y') - \mu_c(x, y)$ if $\mu_c(x, y) < \mu_c(x', y')$.
 - Send a signal B_i that splits μ_c to $(1 - \lambda)\mu_c + \lambda\mu_0$ and $(1 + \lambda)\mu_c - \lambda\mu_0$;
- If $\mu_c \in (\mu, \mu_1]$, then
 - Set λ to be the largest value in $[0, 1]$ satisfying
 - $\lambda \max_{xy} \frac{|\mu_c(x, y) - \mu_1(x, y)|}{\mu_c(x, y)} \leq \varepsilon$, and
 - $\lambda |\mu_1(x, y) - \mu_1(x', y') - \mu_c(x, y) + \mu_c(x', y')| \leq \mu_c(x', y') - \mu_c(x, y)$ if $\mu_c(x, y) < \mu_c(x', y')$.
 - Send a signal B_i that splits μ_c to $(1 - \lambda)\mu_c + \lambda\mu_1$ and $(1 + \lambda)\mu_c - \lambda\mu_1$;
- Update μ_c to the current distribution;
- Increase i ;

Note that every signal B_i sent in the above protocol is ε -weak and non-crossing. Indeed, if B_i splits μ_c into $(1 - \lambda)\mu_c + \lambda\mu_0$ and $(1 + \lambda)\mu_c - \lambda\mu_0$, then

$$\begin{aligned} |\Pr[B_i = 0|xy] - \Pr[B_i = 1|xy]| &= \left| \frac{\mu_c(xy|B_i = 0)}{2\mu_c(xy)} - \frac{\mu_c(xy|B_i = 1)}{2\mu_c(xy)} \right| \\ &= \lambda \frac{|\mu_c(xy) - \mu_0(xy)|}{\mu_c(xy)}, \end{aligned}$$

and the choice of λ guarantees that this is bounded by ε . The same calculation shows the ε -weakness for $\mu_c \in [\mu, \mu_1]$. It can also be easily verified that the signal is non-crossing.

To see that this sequence terminates with probability 1, define

$$\begin{aligned} \Omega = \{ \nu \in [\mu_0, \mu_1] : \exists (x, y), (x', y') \text{ s.t. } \nu(x, y) = \nu(x', y'), \\ \text{while } \mu_0(x, y) \neq \mu_0(x', y') \text{ or } \mu_1(x, y) \neq \mu_1(x', y') \} \end{aligned}$$

and notice that Ω is a finite set. Consider $\mu_c \in [\mu_0, \mu]$. If the value of λ is set by the first condition, then there is a uniform lower-bound for λ :

$$\lambda \geq \lambda_0 := \varepsilon / \max_{xy} \frac{|\mu(x, y) - \mu_0(x, y)|}{\mu(x, y)} = \varepsilon / \max_{xy} \frac{|\mu(x, y) - \mu_1(x, y)|}{\mu(x, y)} > 0.$$

Moreover if λ is set by the other condition, then it means $\mu_c(x, y) < \mu_c(x', y')$, and at least one of $\mu_c|_{B_i=0}$ or $\mu_c|_{B_i=1}$ belongs to Ω . Hence starting at any point μ_c , the random walk terminates with probability at least $2^{-\lceil 1/\lambda_0 \rceil + |\Omega|}$ after $\lceil 1/\lambda_0 \rceil + |\Omega|$ steps. It follows that with probability 1, the random walk terminates. \square

4.2 Proofs of Theorem 5

We present the proof for the internal case only as the external case is similar.

Lemma 5. *Let $w, \delta(\mu)$ and C be as in Theorem 5, and suppose C satisfies Conditions (i), (ii) and (iii). Let τ be a protocol that terminates with probability 1, and further assume τ is in normal form and every signal sent in τ is ε -weak. Given a probability distribution $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$, for every node u in the protocol tree of τ , let μ_u be the probability distribution conditioned on the event that the protocol reaches u . If μ satisfies $w(\delta(\mu_u)) \geq \varepsilon$ for every internal node u , then*

$$C(\mu) \leq \mathbb{IC}_\mu(\tau) + \mathbb{E}_\ell[C(\mu_\ell)],$$

where the expected value is over all leaves ℓ of τ chosen according to the distribution (on the leaves) when the inputs are sampled according to μ .

Proof. For every internal node u , the assumption in the statement of the lemma implies that the signal sent from u is $w(\delta(\mu_u))$ -weak. Hence Condition (iii) shows that the claim is true if τ is a 1-bit protocol, and thus by a simple induction (See [BGPW13, Lemma 5.6]) it is true if τ is a c -bit protocol for any $c < \infty$.

Now assume τ has infinite depth. Consider a large integer c , obtain τ_c by truncating τ after c bits of communication, trivially $\text{IC}_\mu(\tau_c) \leq \text{IC}_\mu(\tau)$. Let G_c denote the set of the leaves of τ_c in which the protocol is forced to terminate. Let \mathcal{L}_c be the set of leaves in τ with depth at most c . Clearly, the set of leaves in τ_c is exactly $G_c \cup \mathcal{L}_c$. As τ_c has a bounded depth, we have

$$C(\mu) \leq \text{IC}_\mu(\tau_c) + \mathbb{E}_{\ell \in \mathcal{L}_c \cup G_c} [C(\mu_\ell)] \leq \text{IC}_\mu(\tau) + \mathbb{E}_{\ell \in \mathcal{L}_c \cup G_c} [C(\mu_\ell)].$$

Let Π_c denote the transcript of τ_c . As τ terminates with probability 1, given any $\alpha > 0$, one can guarantee $\Pr[\Pi_c(xy) \in G_c] < \alpha$ for every xy by choosing c to be sufficiently large. Hence

$$C(\mu) \leq \text{IC}_\mu(\tau) + \mathbb{E}_{\ell \in \mathcal{L}_c} [C(\mu_\ell)] + \alpha \log(|\mathcal{X} \times \mathcal{Y}|).$$

Taking the limit $\alpha \rightarrow 0$ shows $C(\mu) \leq \text{IC}_\mu(\tau) + \mathbb{E}_{\ell \in \mathcal{L}} [C(\mu_\ell)]$ where \mathcal{L} is the set of all leaves of τ . \square

Proof of Theorem 5. Firstly by (ii), $\delta(\mu) = 0$ implies $C(\mu) = \text{IC}_\mu(f) \leq \text{IC}_\mu(f)$. Hence assume $\delta(\mu) > 0$. Consider an arbitrary signal B sent by Alice. As we discussed before, one can interpret B as a one step random walk that starts at μ and jumps either to μ_0 or to μ_1 with corresponding probabilities $\Pr[B = 0|X = x]$ and $\Pr[B = 1|X = x]$. The idea behind the proof is to use Lemma 4 to simulate this random jump with a random walk that has smaller steps so that we can apply the concavity assumption of the theorem to those steps.

Let π be a protocol that computes $[f, 0]$. For $0 < \eta < \delta(\mu)$, applying Lemma 4 one gets a new protocol $\tilde{\pi}$ by replacing every signal sent in π with a random walk consisting of $w(\eta)$ -weak non-crossing unbiased signals. Note $\tilde{\pi}$ terminates with probability 1. Moreover, since $\tilde{\pi}$ is a perfect simulation of π , by Proposition 1 we have $\text{IC}_\mu(\pi) = \text{IC}_\mu(\tilde{\pi})$.

For every node v in the protocol tree of $\tilde{\pi}$, let μ_v be the measure μ conditioned on the event that the protocol reaches the node v . Obtain τ from $\tilde{\pi}$ by terminating at every node v that satisfies $\delta(\mu_v) \leq \eta$. Note that by the construction, Condition (iii) is satisfied on every internal node v of τ , as every such node satisfies $\eta < \delta(\mu_v)$, thus $w(\eta) \leq w(\delta(\mu_v))$ implying the signal sent on node v is $w(\delta(\mu_v))$ -weak. Hence by Lemma 5,

$$C(\mu) \leq \text{IC}_\mu(\tau) + \mathbb{E}_\ell [C(\mu_\ell)],$$

where the expected value is over all leaves of τ . For every μ_ℓ , let $\mu'_\ell \in \Omega$ be a distribution such that $\delta(\mu_\ell) = |\mu_\ell - \mu'_\ell|$. By Conditions (i) and (ii), and the uniform continuity of $\text{IC}_\mu(f)$, we have that for every $\varepsilon > 0$ there exists $\eta > 0$, such that for all μ_ℓ , as long as $\delta(\mu_\ell) = |\mu_\ell - \mu'_\ell| \leq \eta$, then

$$C(\mu_\ell) \leq C(\mu'_\ell) + \varepsilon = \text{IC}_{\mu'_\ell}(f) + \varepsilon \leq \text{IC}_{\mu_\ell}(f) + \varepsilon + \varepsilon = \text{IC}_{\mu_\ell}(f) + 2\varepsilon.$$

As a result,

$$C(\mu) \leq \text{IC}_\mu(\tau) + \mathbb{E}_\ell [\text{IC}_{\mu_\ell}(f) + 2\varepsilon] = \text{IC}_\mu(\tau) + \mathbb{E}_\ell [\text{IC}_{\mu_\ell}(f)] + 2\varepsilon.$$

Since μ_ℓ is generated by truncating $\tilde{\pi}$, we have

$$\text{IC}_\mu(\tau) + \mathbb{E}_\ell[\text{IC}_{\mu_\ell}(f)] \leq \text{IC}_\mu(\tilde{\pi}) = \text{IC}_\mu(\pi).$$

Therefore $C(\mu) \leq \text{IC}_\mu(\pi) + 2\varepsilon$. As this holds for arbitrary ε , we must have $C(\mu) \leq \text{IC}_\mu(\pi)$. \square

5 The multiparty AND function in the number-in-hand model

In [BGPW13] it is shown that in the two-player setting, a certain (unconventional) protocol that we refer to as the buzzers protocol, has optimal information and external information cost for the 2-bit AND function. In this section we show that the buzzers protocol can be generalized to an optimal protocol for the multiparty AND function in the number-in-hand model (assuming Assumption 1).

For the sake of brevity, we denote $\mu_x := \mu(\{x\})$ for every $x \in \{0, 1\}^k$. Furthermore we assume that $\mu_{e_1} \leq \dots \leq \mu_{e_k}$. The protocol is given by having buzzers with waiting times which have independent exponential distributions, and start at times t_1, \dots, t_k for players $1, \dots, k$, respectively. Although the protocol π_μ^\wedge described in Figure 1 is not a conventional communication protocol, it can be easily approximated by discretization and truncation of time.

Fig. 1. The protocol π_μ^\wedge for solving the AND function on a distribution μ .

- There is a clock whose time starts at 0 and increases continuously to $+\infty$.
- Let $t_i := \ln \frac{\mu_{e_i}}{\mu_{e_1}}$ for $i = 1, \dots, k$, and let $t_{k+1} := \infty$.
- For every $i = 1, \dots, k$, if $x_i = 0$, then the i -th player privately picks an independent random variable T_i with exponential distribution, and if time reaches $t_i + T_i$, the player announces that his/her input is 0, and the protocol terminates immediately with all the players knowing that $\bigwedge_{i=1}^k x_i = 0$.
- If the clock reaches $+\infty$ without any player announcing their input, the players will know that $\bigwedge_{i=1}^k x_i = 1$.

Recall that the exponential distribution is memoryless, and intuitively can be generated in the following manner: Consider a buzzer starting at time $t = 0$. At every infinitesimal time interval of length dt , independently of the past, it buzzes with probability dt , and then stops. The waiting time for a buzz to happen has exponential distribution.

Thus we can describe π_μ^\wedge as in the following: For every $i \in [k]$, if $x_i = 0$, the i -th player activates a buzzer at time t_i . When the first buzz happens the

protocol terminates, and the players decide that $\bigwedge_{i=1}^k x_i = 0$. If the time reaches ∞ without anyone buzzing, they decide $\bigwedge_{i=1}^k x_i = 1$. In Theorem 6 we show that for the measures μ that satisfy Assumption 1, the protocol π_μ^\wedge has optimal external and internal information cost.

Theorem 6 (Main Theorem 2). *For every μ satisfying Assumption 1, the protocol π_μ^\wedge has the smallest external and internal information cost.*

In order to prove Theorem 6, we need to verify that the concavity conditions of Theorem 5 are satisfied. Consider the measure μ that is uniformly distributed over e_1, \dots, e_k . That is $\mu_0 = 0$ and $\mu_{e_1} = \dots = \mu_{e_k} = 1/k$. Note that when the protocol π^\wedge is executed on this measure, all the players become active at time 0, and as time proceeds, they do not obtain any new information about the inputs of the other players until one of the players buzzes. Then at that point the input is revealed to all the players. Due to this discrete nature of the corresponding random-walk on $\Delta(\mathcal{X} \times \mathcal{Y})$, we need to analyze this particular measure separately, and afterwards when verifying the concavity conditions, we can let Ω in the statement of Theorem 5 include this measure. Claim 1 below verifies Theorem 6 for this particular measure.

Claim 1. *Let μ be the measure that $\mu_0 = 0$ and $\mu_{e_1} = \dots = \mu_{e_k} = 1/k$. The internal and external information cost of the protocol π^\wedge is optimal with respect to μ .*

Proof. First we present the proof for the external information complexity. Let π be any protocol that solves the multi-party AND function correctly, and let t be a possible transcript of the protocol. First note that it is not possible to have $\Pr[\Pi_{e_m} = t] > 0$ for all $1 \leq m \leq k$. Indeed by rectangle property this would imply $\Pr[\Pi_1 = t] > 0$, and since the correct output for $\mathbf{1}$ is different from that of e_1, \dots, e_k , we would get a contradiction with the assumption that π solves AND correctly on all inputs. Hence to every transcript t , we can assign a $j(t) \in \{1, \dots, m\}$ with $\Pr[\Pi_{e_j} = t] = 0$. Now for a random $X \sim \mu$, denote $J = j(\Pi_X)$, and notice that conditioned on $J = j$, X is supported on the set $\{e_1, \dots, e_k\} \setminus \{e_j\}$ of size $k-1$, and thus $H(X|J) \leq \log(k-1)$. Consequently, we have

$$\text{IC}_\mu^{\text{ext}}(\pi) = I(X; \Pi_X) = I(X; \Pi_X J) \geq I(X; J) = H(X) - H(X|J) \geq \log k - \log(k-1).$$

On the other hand, consider our protocol π_μ^\wedge . Note that under μ , all players are activated at the same time, and consequently by symmetry, for every termination time τ and player $j \in \{1, \dots, k\}$, the random variable $X|_{\Pi_X=(\tau, j)}$ is uniformly distributed on $\{e_1, \dots, e_k\} \setminus \{e_j\}$. Hence $H(X|\Pi_X) = \log(k-1)$. We conclude that

$$\text{IC}_\mu^{\text{ext}}(\pi^\wedge) = I(X; \Pi_X) = H(X) - H(X|\Pi_X) = \log k - \log(k-1).$$

Next we turn to the internal case. Again, let π be any protocol that solves the multi-party AND correctly, and let J be defined as above. First note that for

$i \in [k]$, $X|_{X_i=1}$ is supported on the single point $\{e_i\}$ and $X|_{X_i=0}$ is uniformly distributed on $\{e_1, \dots, e_k\} \setminus \{e_i\}$. Hence

$$H(X|X_i) = \frac{1}{k} H(X|X_i=1) + \frac{k-1}{k} H(X|X_i=0) = \frac{k-1}{k} \log(k-1).$$

Moreover for $i, j \in [k]$, $X|_{J=j, X_i=0}$ is supported on $\{e_1, \dots, e_k\} \setminus \{e_i, e_j\}$. Hence using $\mathbf{Pr}[J=i] = \mathbf{Pr}[J=i, X_i=0]$, we have

$$\begin{aligned} H(X|JX_i) &= \sum_{j=1}^k \mathbf{Pr}[J=j, X_i=0] H(X|_{J=j, X_i=0}) \\ &\leq \sum_{j=1}^k \mathbf{Pr}[J=j, X_i=0] \log |\{e_1, \dots, e_k\} \setminus \{e_i, e_j\}| \\ &= \frac{k-1}{k} \log(k-2) + \mathbf{Pr}[J=i] (\log(k-1) - \log(k-2)). \end{aligned}$$

Summing over i , we obtain

$$\sum_{i=1}^k H(X|JX_i) = (k-2) \log(k-2) + \log(k-1),$$

and thus

$$\begin{aligned} \text{IC}_\mu(\pi) &= \sum_{i=1}^k I(X; \Pi_X | X_i) = \sum_{i=1}^k I(X; \Pi_X J | X_i) \\ &\geq \sum_{i=1}^k I(X; J | X_i) = \sum_{i=1}^k H(X|X_i) - H(X|JX_i) \\ &\geq (k-1) \log(k-1) - ((k-2) \log(k-2) + \log(k-1)) \\ &= (k-2) (\log(k-1) - \log(k-2)). \end{aligned}$$

On the other hand, for the protocol π_μ^\wedge , by symmetry, for every termination time τ and player $j \in \{1, \dots, k\}$, the random variable $X|_{\Pi_X=(\tau, j), X_i=0}$ is uniformly distributed on $\{e_1, \dots, e_k\} \setminus \{e_j, e_i\}$. Hence

$$H(X|\Pi_X X_i) = \frac{1}{k} \log(k-1) + \frac{k-2}{k} \log(k-2).$$

We conclude that

$$\begin{aligned} \text{IC}_\mu(\pi^\wedge) &= \sum_{i=1}^k I(X; \Pi_X | X_i) = (k-1) \log(k-1) - \sum_{i=1}^k H(X|\Pi_X X_i) \\ &= (k-2) (\log(k-1) - \log(k-2)). \end{aligned} \quad \square$$

Claim 2. *It suffices to verify Theorem 6 for measures μ with $\mu(1) = 0$.*

Proof. Let μ be a measure satisfying Assumption 1, and let π be a protocol that solves the multiparty AND function correctly on all the inputs. Let Π denote the transcript of this protocol, and let $B = 1_{[X=1]}$. Since π solves the AND function correctly, Π determines the value of B . We have

$$\begin{aligned} \text{IC}_\mu^{\text{ext}}(\pi) &= \text{I}(X; \Pi_X) = \text{I}(XB_X; \Pi_X) = \text{I}(B_X; \Pi_X) + \text{I}(X; \Pi_X | B_X) \\ &= 0 + \Pr[X = 1] \text{I}(X; \Pi_X | X = 1) + \Pr[X \neq 1] \text{I}(X; \Pi_X | X \neq 1) \\ &= \Pr[X \neq 1] \text{I}(X; \Pi_X | X \neq 1) = (1 - \mu_1) \text{IC}_{\mu'}^{\text{ext}}(\pi), \end{aligned}$$

where μ' is the measure μ conditioned on the event that the input is not equal to 1. Similarly

$$\text{IC}_\mu(\pi) = (1 - \mu_1) \text{IC}_{\mu'}(\pi).$$

Finally, to conclude the claim, note that π_μ^\wedge and $\pi_{\mu'}^\wedge$ are identical as $\mu_{e_i}/\mu_{e_1} = \mu'_{e_i}/\mu'_{e_1}$ for all $i = 1, \dots, k$. \square

6 Proof of Theorem 6

In this section we prove Theorem 6 by verifying the concavity conditions of Theorem 5. Let μ be a measure satisfying Assumption 1, and $X = (X_1, \dots, X_k)$ denote the random k -bit input. Let Π be the random variable corresponding to the transcript of the protocol π_μ^\wedge . Let $\Pi_x = \Pi|_{X=x}$.

To verify the concavity condition, we consider a signal B with parameter ε sent by the player s . That is

$$\Pr[B = 0 | X_s = 0] = \frac{1 + \varepsilon \Pr[X_s = 1]}{2},$$

and

$$\Pr[B = 1 | X_s = 1] = \frac{1 + \varepsilon \Pr[X_s = 0]}{2}.$$

Note that $\Pr[B = 0] = \Pr[B = 1] = \frac{1}{2}$, i.e., the signal B is unbiased. Let μ^0 and μ^1 respectively denote the distributions of $X^0 := X|_{B=0}$ and $X^1 := X|_{B=1}$. We have $\mu = \frac{\mu^0 + \mu^1}{2}$. Let Π^0 and Π^1 denote the random variables corresponding to the transcripts of $\pi_{\mu^0}^\wedge$ and $\pi_{\mu^1}^\wedge$, respectively.

Note that the transcript of π_μ^\wedge contains the termination time t , and if $t < \infty$, also the name of the player who first buzzed. We denote by π_∞ the transcript corresponding to termination time $t = \infty$, and by π_t^m the termination time $t < \infty$ with the m -th player buzzing.

For $t \in [0, \infty)$, let $\Phi_x(t)$ denote the total amount of active time spent by all players before time t if the input is x . For $t_r \leq t < t_{r+1}$, we have

$$\Phi_x(t) = \sum_{i: x_i=0} \max(t - t_i, 0) = \sum_{i \in [1, r], x_i=0} t - t_i.$$

The probability density function f_x of Π_x is given by

$$f_x(\pi_t^m) = \begin{cases} 0 & t_m > t \text{ or } x_m = 1 \\ e^{-\Phi_x(t)} & \text{otherwise} \end{cases},$$

and $\Pr(\Pi_1 = \pi_\infty) = 1$. The distribution of the transcript Π is then

$$f(\pi_t^m) = \sum_x \mu_x f_x(\pi_t^m).$$

Define f^0 , f_x^0 and f^1 , f_x^1 analogously for $\pi_{\mu^0}^\wedge$ and $\pi_{\mu^1}^\wedge$, respectively.

6.1 Probability distributions μ^0 and μ^1

Denote $\beta_s := \Pr[X_s = 1]$, and $\zeta_s := \Pr[X_s = 0]$. For $B = 0$, we have,

$$\mu_x^0 = \begin{cases} (1 + \varepsilon \Pr[x_s = 1])\mu_x = (1 + \varepsilon \beta_s)\mu_x & x_s = 0 \\ (1 - \varepsilon \Pr[x_s = 0])\mu_x = (1 - \varepsilon \zeta_s)\mu_x & x_s = 1 \end{cases}$$

Consequently, the new starting times are $t_i^0 = t_i$ for $i \neq s$, and $t_s^0 = t_s - \gamma_0$ where

$$\gamma_0 = \ln \left(\frac{1 + \varepsilon \beta_s}{1 - \varepsilon \zeta_s} \right). \quad (13)$$

Hence

$$\mu_x^0 f_x^0(\pi_t^m) = \begin{cases} \mu_x^0 f_x(\pi_t^m) & t < t_s - \gamma_0 \\ (1 + \varepsilon \beta_s)\mu_x f_x(\pi_t^m) e^{-(t - t_s + \gamma_0)} & t \in [t_s - \gamma_0, t_s), x_s = 0, m \neq s \\ (1 - \varepsilon \zeta_s)\mu_x f_x(\pi_t^m) & t \in [t_s - \gamma_0, t_s), x_s = 1, m \neq s \\ \mu_x^0 f_x^0(\pi_t^s) & t \in [t_s - \gamma_0, t_s), m = s \\ (1 - \varepsilon \zeta_s)\mu_x f_x(\pi_t^m) & t \geq t_s \end{cases}$$

On the other hand, for $B = 1$, we have,

$$\mu_x^1 = \begin{cases} (1 - \varepsilon \beta_s)\mu_x & x_s = 0 \\ (1 + \varepsilon \zeta_s)\mu_x & x_s = 1 \end{cases}$$

Consequently the new starting times are $t_i^1 = t_i$ for $i \neq s$, and $t_s^1 = t_s + \gamma_1$ where

$$\gamma_1 = \ln \left(\frac{1 + \varepsilon \zeta_s}{1 - \varepsilon \beta_s} \right). \quad (14)$$

Hence when $m \neq s$,

$$\mu_x^1 f_x^1(\pi_t^m) = \begin{cases} \mu_x^1 f_x(\pi_t^m) & t \leq t_s \\ (1 - \varepsilon \beta_s)\mu_x f_x(\pi_t^m) e^{t - t_s} & t \in [t_s, t_s + \gamma_1), x_s = 0 \\ (1 + \varepsilon \zeta_s)\mu_x f_x(\pi_t^m) & t \in [t_s, t_s + \gamma_1), x_s = 1 \\ (1 + \varepsilon \zeta_s)\mu_x f_x(\pi_t^m) & t \geq t_s + \gamma_1 \end{cases}$$

For $m = s$,

$$\mu_x^1 f_x^1(\pi_t^s) = \begin{cases} (1 + \varepsilon \zeta_s)\mu_x f_x(\pi_t^s) & t > t_s + \gamma_1 \text{ and } x_s = 0 \\ 0 & \text{otherwise.} \end{cases}$$

6.2 Setting up and first reductions

We set Ω to be the set of all external (resp. internal) trivial measures together with the measure in Claim 1, and in the external case we set $w(x) = ck^{-20}x^4$ for some fixed constant $c > 0$ (one may need to pick a different $w(x)$ for internal case). Using the memoryless property of exponential distribution, we can shift the activation time of all the players by $-\ln(\mu_{e_s}/\mu_{e_1})$, and assume that $t_1 = -\ln(\mu_{e_s}/\mu_{e_1}), \dots, t_s = 0, \dots, t_k = \ln(\mu_{e_k}/\mu_{e_s})$.

Let $\phi(x) := x \ln(x)$. Using the notion of concealed information from Section 3.2, the concavity conditions of Theorem 5 reduce to verifying

$$\begin{aligned} & \int_{-\infty}^{\infty} \sum_m \left(\phi(f(\pi_t^m)) - \frac{\phi(f^0(\pi_t^m)) + \phi(f^1(\pi_t^m))}{2} \right) \\ & - \sum_m \sum_x \left(\phi(\mu_x f_x(\pi_t^m)) - \frac{\phi(\mu_x^0 f_x^0(\pi_t^m)) + \phi(\mu_x^1 f_x^1(\pi_t^m))}{2} \right) dt \geq 0, \end{aligned} \quad (15)$$

for the external case, and

$$\begin{aligned} & \sum_{j=1}^k \int_{-\infty}^{\infty} \sum_m \sum_{b=0}^1 \left(\phi(f_{x_j=b}(\pi_t^m)) - \frac{\phi(f_{x_j=b}^0(\pi_t^m)) + \phi(f_{x_j=b}^1(\pi_t^m))}{2} \right) \\ & - \sum_m \sum_x \left(\phi(\mu_x f_x(\pi_t^m)) - \frac{\phi(\mu_x^0 f_x^0(\pi_t^m)) + \phi(\mu_x^1 f_x^1(\pi_t^m))}{2} \right) dt \geq 0, \end{aligned} \quad (16)$$

for the internal case, where

$$f_{x_j=b}(\pi_t^m) := \sum_{X: X_j=b} \mu_X f_X(\pi_t^m),$$

and

$$f_{x_j=b}^0(\pi_t^m) := \sum_{X: X_j=b} \mu_X^0 f_X^0(\pi_t^m), \quad f_{x_j=b}^1(\pi_t^m) := \sum_{X: X_j=b} \mu_X^1 f_X^1(\pi_t^m).$$

Denote the function inside the integral of (16) by $\text{concav}_\mu(t, j)$, and the function inside the integral of (15) by $\text{concav}_\mu^{ext}(t)$. Note further that by Claim 2 we can assume that $\mu_1 = 0$. Hence our goal reduces to show the following:

Statement 1 (First reduction). *To prove Theorem 6 it suffices to assume μ satisfies $\mu(1) = 0$, and verify*

$$\int_{-\infty}^{\infty} \text{concav}_\mu^{ext}(t) dt \geq 0 \quad \text{and} \quad \sum_{j=1}^k \int_{-\infty}^{\infty} \text{concav}_\mu(t, j) dt \geq 0.$$

Recall we assumed $t_s = 0$ by shifting the time. The next two claims show that one only needs to focus on the interval $[-\gamma_0, \gamma_1]$.

Claim 3. We have $\int_{-\infty}^{-\gamma_0} \text{concav}_{\mu}^{ext}(t)dt \geq 0$ and $\sum_{j=1}^k \int_{-\infty}^{-\gamma_0} \text{concav}_{\mu}(t, j)dt \geq 0$.

Proof. Observe that Π, Π^0 and Π^1 are identical up to time $-\gamma_0$. Let Π_P denote a similar protocol, with the only difference that in Π_P at time $t = -\gamma_0$ all the players reveal their inputs. Then,

$$\int_{-\infty}^{-\gamma_0} \text{concav}_{\mu}^{ext}(t)dt = H(X|\Pi_P) - H(X|\Pi_P, B) \geq 0,$$

and

$$\sum_{j=1}^k \int_{-\infty}^{-\gamma_0} \text{concav}_{\mu}(t, j)dt = \sum_{j=1}^k (H(X|X_j, \Pi_P) - H(X|X_j, \Pi_P, B)) \geq 0. \quad \square$$

Claim 4. We have $\int_{\gamma_1}^{\infty} \text{concav}_{\mu}^{ext}(t)dt = 0$ and $\sum_{j=1}^k \int_{\gamma_1}^{\infty} \text{concav}_{\mu}(t, j)dt = 0$.

Proof. We use the formula in (15) by integrating in the corresponding range $[\gamma_1, \infty)$. As $t \geq \gamma_1$, plug in $\mu_x^0 f_x^0(\pi_t^m) = (1 - \varepsilon \zeta_s) \mu_x f_x(\pi_t^m)$ and $\mu_x^1 f_x^1(\pi_t^m) = (1 + \varepsilon \zeta_s) \mu_x f_x(\pi_t^m)$, a simple calculation shows $\int_{\gamma_1}^{\infty} \text{concav}_{\mu}^{ext}(t)dt = 0$. Similarly one can calculate the internal case. \square

Statement 2 (Second reduction). To prove Theorem 6 it suffices to assume μ satisfies $\mu(\mathbf{1}) = 0$, and verify

$$\int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}^{ext}(t)dt \geq 0 \quad \text{and} \quad \sum_{j=1}^k \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j)dt \geq 0.$$

Remark 4. The computation result of the two-party AND done in [BGPW13, Section 7.7] shows the concavity term (the one that we want to verify its non-negativity) can be of order ε^2 . One will see in Section 6.4 that our computation gives only an order ε^3 . This is because we choose to focus our computation, as allowed by Statement 2, on the interval $[-\gamma_0, \gamma_1]$ only. Claim 5 below shows an order ε^2 term can appear if the whole range is considered.

Claim 5. Suppose $s \geq 2$ and $L = |t_{s-1}| > 0$. If $\gamma_0 \leq L/2$, then

$$\int_{t_{s-1}}^{-\gamma_0} \text{concav}_{\mu}^{ext}(t)dt \geq \frac{(1 - e^{-(s-1)L/2})\mu_0 \mu_{e_s}}{2(s-1)} \varepsilon^2 \geq 0, \quad (17)$$

and

$$\sum_{j=1}^k \int_{t_{s-1}}^{-\gamma_0} \text{concav}_{\mu}(t, j)dt \geq \frac{(k-1)(1 - e^{-(s-1)L/2})\mu_0 \mu_{e_s}}{2(s-1)} \varepsilon^2 \geq 0. \quad (18)$$

Proof. Consider external case first. Let μ' be defined as

$$\mu'_x = \begin{cases} \beta \mu_x, & x_s = 0, \\ -\zeta \mu_x, & x_s = 1. \end{cases}$$

Then $\mu^0 = \mu + \varepsilon\mu'$ and $\mu^1 = \mu - \varepsilon\mu'$, hence $f^0(\pi_t^m) = f(\pi_t^m) + \varepsilon \sum \mu'_x f_x(\pi_t^m)$ and $f^1(\pi_t^m) = f(\pi_t^m) - \varepsilon \sum \mu'_x f_x(\pi_t^m)$. Note that $f(\pi_t^m) = 0$ (in our case this happens when $m \geq s$) implies $\text{concav}_\mu^{ext}(t) = 0$. On the other hand, when $f(\pi_t^m) \neq 0$ (i.e., $1 \leq m \leq s-1$), using Taylor expansion at the point $f(\pi_t^m)$ for functions $\phi(f^0(\pi_t^m))$ and $\phi(f^1(\pi_t^m))$, and expansion at $\mu_x f_x(\pi_t^m)$ for functions $\phi(\mu_x^0 f_x^0(\pi_t^m))$ and $\phi(\mu_x^1 f_x^1(\pi_t^m))$, we obtain (note here we won't have ε^3)

$$\begin{aligned} \text{concav}_\mu^{ext}(t) &\geq \sum_{m=1}^{s-1} \left(\sum_x \frac{(\mu'_x f_x(\pi_t^m))^2}{2\mu_x f_x(\pi_t^m)} - \frac{(\sum \mu'_x f_x(\pi_t^m))^2}{2f(\pi_t^m)} \right) \varepsilon^2 \\ &= \frac{1}{2} \sum_{m=1}^{s-1} \left(\mu_{e_s} f_{e_s}(\pi_t^m) \left(1 - \frac{\mu_{e_s} f_{e_s}(\pi_t^m)}{f(\pi_t^m)} \right) \right) \varepsilon^2 \\ &\geq \frac{1}{2} \sum_{m=1}^{s-1} \left(\mu_{e_s} f_{e_s}(\pi_t^m) \frac{\mu_0 f_0(\pi_t^m)}{f(\pi_t^m)} \right) \varepsilon^2 \geq 0. \end{aligned} \quad (19)$$

By Statement 3 one can assume $\mu_{e_s} = \dots = \mu_{e_k}$ and $\mu_{e_1} = \dots = \mu_{e_{s-1}} = \mu_{e_s} e^{-L}$, thus $\mu_0 = 1 - (k-s+1)\mu_{e_s} - (s-1)\mu_{e_s} e^{-L}$. Then $t_{s-1} = 0$ and $t_s = L$. As $\gamma_0 \leq L/2$ implies $t_s - \gamma_0 = L - \gamma_0 \geq L/2$, and (19) says the integrand is non-negative, hence a lower bound is given by the integration of (19) in the range $[0, L/2]$. For $t \in [0, L/2]$ and $1 \leq m \leq s-1$, we have $f_0(\pi_t^m) = f_{e_s}(\pi_t^m) = \dots = f_{e_k}(\pi_t^m) = e^{-(s-1)t}$, and $f_{e_1}(\pi_t^m) = \dots = f_{e_{s-1}}(\pi_t^m) = e^{-(s-2)t}$, thus $f(\pi_t^m) = (1 - (s-1)\mu_{e_s} e^{-L} + (s-2)\mu_{e_s} e^{-L} e^t) e^{-(s-1)t} \leq (s-1)e^{-(s-1)t}$. Hence,

$$(19) \geq \frac{s-1}{2} \mu_{e_s} f_{e_s} \frac{\mu_0 f_0(\pi_t^m)}{(s-1)e^{-(s-1)t}} \varepsilon^2 = \frac{\mu_0 \mu_{e_s}}{2} e^{-(s-1)t} \varepsilon^2.$$

Integrating in the range $[0, L/2]$ with respect to t gives the desired bound (17).

Similarly, in the internal case one has

$$\begin{aligned} \sum_{j=1}^k \text{concav}_\mu(t, j) &\geq \frac{1}{2} \sum_{m=1}^{s-1} \sum_{j=1, j \neq s}^k \left(\mu_{e_s} f_{e_s}(\pi_t^m) \frac{\mu_0 f_0(\pi_t^m)}{f(\pi_t^m) - \mu_{e_j} f_{e_j}(\pi_t^m)} \right) \varepsilon^2 \\ &\geq \frac{k-1}{2} \sum_{m=1}^{s-1} \left(\mu_{e_s} f_{e_s}(\pi_t^m) \frac{\mu_0 f_0(\pi_t^m)}{f(\pi_t^m)} \right) \varepsilon^2. \end{aligned}$$

Hence we get the bound (18) after integration. \square

6.3 Futher reductions

In this section we obtain a futher reduction of Statement 2 that will have a constant number of variables and so one can finally verify it using Wolfram Mathematica:

Statement 3 (Third reduction). *To prove Theorem 6 it suffices to assume μ satisfies*

$$\mu_{e_1} = \dots = \mu_{e_{s-1}} = \beta, \quad \mu_{e_s} = \dots = \mu_{e_k} = e^{\gamma_0} \beta, \quad \mu_0 = 1 - (s-1)\beta - (k-s+1)e^{\gamma_0} \beta, \quad (20)$$

where $0 < \beta < 1$, and verify

$$\int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}^{\text{ext}}(t) dt \geq 0 \quad \text{and} \quad \sum_{j=1}^k \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j) dt \geq 0.$$

Statement 3 follows from Claim 7 showing that it suffices to consider measures μ such that $\mu_{e_j} = \mu_{e_s}$ for all $j \geq s$, together with the observation that conditioned on the buzz time $t \in [-\gamma_0, \gamma_1]$, we have $\mu_{e_1}|_{t \geq t_s - \gamma_0} = \dots = \mu_{e_{s-1}}|_{t \geq t_s - \gamma_0}$.

Claim 6. For every z ,

$$\begin{aligned} & \Pr[X = z \wedge t(\Pi_z) \in [-\gamma_0, \gamma_1]] \\ &= \frac{\Pr[X^0 = z \wedge t(\Pi_z^0) \in [-\gamma_0, \gamma_1]] + \Pr[X^1 = z \wedge t(\Pi_z^1) \in [-\gamma_0, \gamma_1]]}{2}. \end{aligned}$$

Proof. We need to show

$$\mu_z \sum_m \int_{-\gamma_0}^{\gamma_1} f_z(\pi_t^m) dt = \frac{1}{2} \left(\mu_z^0 \sum_m \int_{-\gamma_0}^{\gamma_1} f_z^0(\pi_t^m) dt + \mu_z^1 \sum_m \int_{-\gamma_0}^{\gamma_1} f_z^1(\pi_t^m) dt \right).$$

Recall that $\Phi_z(t)$ denotes the total amount of active time spent by all players before time t . The probability that Π_z finishes in the interval $[-\gamma_0, \gamma_1]$ is equal to

$$e^{-\Phi_z(-\gamma_0)} - e^{-\Phi_z(\gamma_1)}.$$

Denoting by $\Phi_z^0(t)$ and $\Phi_z^1(t)$ the total active time for the protocols $\pi_{\mu_0}^{\wedge}$ and $\pi_{\mu_1}^{\wedge}$ on the input z , the claim is equivalent to

$$\mu_z \cdot (e^{-\Phi_z(-\gamma_0)} - e^{-\Phi_z(\gamma_1)}) = \frac{\mu_z^0 \cdot (e^{-\Phi_z^0(-\gamma_0)} - e^{-\Phi_z^0(\gamma_1)})}{2} + \frac{\mu_z^1 \cdot (e^{-\Phi_z^1(-\gamma_0)} - e^{-\Phi_z^1(\gamma_1)})}{2}.$$

Since $\mu_z = \frac{\mu_z^0 + \mu_z^1}{2}$ and $\Phi_z(-\gamma_0) = \Phi_z^0(-\gamma_0) = \Phi_z^1(-\gamma_0)$, the equality reduces to

$$\mu_z e^{-\Phi_z(\gamma_1)} = \frac{\mu_z^0 e^{-\Phi_z^0(\gamma_1)} + \mu_z^1 e^{-\Phi_z^1(\gamma_1)}}{2}.$$

When $z_s = 1$, $\Phi_z = \Phi_z^0 = \Phi_z^1$, and thus $\mu_z = \frac{\mu_z^0 + \mu_z^1}{2}$ verifies the equality. In the case of $z_s = 0$, we have that $\Phi_z^0(\gamma_1) = \Phi_z(\gamma_1) + \gamma_0$, and $\Phi_z^1(\gamma_1) = \Phi_z(\gamma_1) - \gamma_1$. Substituting $\gamma_0 = \ln\left(\frac{1+\varepsilon\beta_s}{1-\varepsilon\zeta_s}\right)$, $\gamma_1 = \ln\left(\frac{1+\varepsilon\zeta_s}{1-\varepsilon\beta_s}\right)$, $\mu_z^0 = (1 + \varepsilon\beta_s)\mu_z$ and $\mu_z^1 = (1 - \varepsilon\beta_s)\mu_z$ verifies the equality. \square

Claim 7. Suppose μ satisfies $\mu_{e_s} = \dots = \mu_{e_{s+a}} < \mu_{e_{s+a+1}}$ for some $a \geq 0$ with $s + a + 1 \leq k$. Assume ε is sufficiently small so that $\gamma_1 \leq t_{s+a+1}$. Let μ' be a measure for the $(s+a)$ -player AND function, defined as: $\mu'_0 = \mu_0 + \sum_{j>s+a} \mu_{e_j}$, and $\mu'_{e_j} = \mu_{e_j}$ for $1 \leq j \leq s+a$. Then the following hold.

$$(1). \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}^{\text{ext}}(t) dt = \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu'}^{\text{ext}}(t) dt;$$

(2). If $\sum_{j=1}^{s+a} \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu'}(t, j) dt \geq 0$, then $\sum_{j=1}^k \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j) dt \geq 0$.

This claim shows that to verify the concavity conditions (15) and (16) it suffices to consider only those measures satisfying $\mu_{e_j} = \mu_{e_s}$ for all $j > s$.

Proof. We confine ourselves in the interval $t \in [-\gamma_0, \gamma_1]$ throughout the proof. Let f, f' and Π, Π' denote the pdf and protocols for π_{μ}^{\wedge} and $\pi_{\mu'}^{\wedge}$, respectively.

(1). Obviously we have

$$f'_{\mathbf{0}}(\pi_t^m) = f_{\mathbf{0}}(\pi_t^m), \quad \text{and} \quad f'_{e_j}(\pi_t^m) = f_{e_j}(\pi_t^m), \quad 1 \leq j \leq s + a. \quad (21)$$

For the protocol π_{μ}^{\wedge} , observe we have

$$f_{\mathbf{0}}(\pi_t^m) = f_{e_j}(\pi_t^m), \quad j > s + a, \quad (22)$$

for all $m = 1, \dots, k$. Hence (21) and (22) imply that $f(\pi_t^m) = f'(\pi_t^m)$. Clearly similar results hold for Π^0, Π^1 and Π'^0, Π'^1 . This imply that the first integral in (15) does not change from μ to μ' .

It remains to show that the second integral in (15) does not change either. Expand this integral gives,

$$\begin{aligned} & \int_{-\gamma_0}^{\gamma_1} \sum_X \sum_m \left(f_X(\pi_t^m) \mu_X \log(\mu_X) - \frac{\mu_X^0 f_X^0(\pi_t^m) \log(\mu_X) + \mu_X^1 f_X^1(\pi_t^m) \log(\mu_X)}{2} \right) dt \\ & + \int_{-\gamma_0}^{\gamma_1} \sum_X \sum_m \left(\mu_X \phi(f_X(\pi_t^m)) - \frac{\mu_X^0 (\phi(f_X^0(\pi_t^m)) + f_X^0(\pi_t^m) \log(1 + \varepsilon\beta)) + \mu_X^1 (\phi(f_X^1(\pi_t^m)) + f_X^1(\pi_t^m) \log(1 - \varepsilon\beta))}{2} \right) dt. \end{aligned} \quad (23)$$

By Claim 6 the first integral in (23) is 0. Hence it only remains to show the second integral in (23) does not change. But this is again a direct consequence of (21) and (22) with corresponding facts for Π_X^0 and Π_X^1 .

(2). By definition of the measures μ, μ' , one has

$$\sum_{j=1}^k \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j) dt - \sum_{j=1}^{s+a} \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu'}(t, j) dt = \sum_{j=s+a+1}^k \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j) dt.$$

Hence it suffices to show $\sum_{j=s+a+1}^k \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j) dt \geq 0$.

Let $\mu_{X_j=b}$ denote the distribution μ of X conditioned on $X_j = b$, one can check that

$$\int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j) dt = \mathbb{E}_b \int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu_{X_j=b}}^{ext}(t) dt. \quad (24)$$

In section 6.4 we show the external concavity condition indeed holds, hence (24) implies $\int_{-\gamma_0}^{\gamma_1} \text{concav}_{\mu}(t, j) dt \geq 0$, as desired. \square

Proof of Theorem 6. We use \wedge to denote the multiparty AND function. Consider the external case first. Recall we set Ω to be the set of all external trivial measures together with the measure in Claim 1, hence Condition (i) and (ii) are satisfied. Picking $w(x) = ck^{-20}x^4$ for some fixed constant $c > 0$, we verify Condition (iii) in Section 6.4. Hence $\text{IC}_\mu^{\text{ext}}(\pi^\wedge) \leq \text{IC}_\mu^{\text{ext}}(\wedge)$, as $\text{IC}_\mu^{\text{ext}}(\pi^\wedge)$ is also an upper bound, hence we proved $\text{IC}_\mu^{\text{ext}}(\pi^\wedge) = \text{IC}_\mu^{\text{ext}}(\wedge)$.

Similarly for the internal case the concavity Condition (iii) is verified in Section 6.4. \square

6.4 Information cost of multiparty AND function

To simplify the notation, since every function has the argument π_t^m , we sometimes omit it from the writing while knowing it was there, such as we write f to mean $f(\pi_t^m)$. We will use μ_0, μ_j, f_0, f_j instead of $\mu_0, \mu_{e_j}, f_0, f_{e_j}$ when there is no ambiguity, similar notations are used for measures μ^0, μ^1 and functions f^0, f^1 .

Taylor expansions Recall $\beta_s = \mu_s$ and $\zeta_s = 1 - \beta_s$. By the claims in Section 6.3, we can assume that

$$\mu_1 = \cdots = \mu_{s-1} = \beta, \quad \mu_s = \cdots = \mu_k = e^{\gamma_0} \beta, \quad \mu_0 = 1 - (s-1)\beta - (k-s+1)e^{\gamma_0} \beta. \quad (25)$$

Observe that $0 < \beta < 1/k$ (the measure when $\beta = 0$ is both external and internal trivial). Furthermore, viewing γ_0 and γ_1 as functions of ε , plugging $\beta_s = e^{\gamma_0} \beta$ and $\zeta_s = 1 - \beta_s = 1 - e^{\gamma_0} \beta$ into (13) and (14), by implicit differentiation, we have

$$\begin{cases} \gamma_0(0) = 0, \gamma_0'(0) = 1, \gamma_0''(0) = 1 - 2\beta, \gamma_0'''(0) = 2 - 10\beta + 8\beta^2; \\ \gamma_1(0) = 0, \gamma_1'(0) = 1, \gamma_1''(0) = 2\beta - 1, \gamma_1'''(0) = 2 + 6\beta^2. \end{cases} \quad (26)$$

These derivatives are used in the Mathematica computation. To simplify the notation we let $\zeta = \zeta_s = 1 - e^{\gamma_0} \beta$.

Assuming $\varepsilon < 1/2$, then $\gamma_0 + \gamma_1 \leq 2 \ln(1 + 2\varepsilon) \leq 4\varepsilon$. Also note $|e^{-x} - 1| \leq x$ for $x \geq 0$, which together with the fact that $\Phi_x(t) \leq k(\gamma_0 + \gamma_1) \leq 4k\varepsilon$ implies the following:

- $\mu_0 f_0(\pi_t^m)$ is either 0 or close to $1 - k\beta$ with distance bounded by $4k\varepsilon$;
- for $j \neq 0$, we have $\mu_j f_j(\pi_t^m)$ is either 0 or close to β with distance bounded by $4(k+1)\varepsilon$;
- $f(\pi_t^m)$ is either 0 or close to $1 - \beta$ with distance bounded by $16k^2\varepsilon$;
- for $j \neq 0$ and $j \neq m$, we have $f(\pi_t^m) - \mu_j f_j(\pi_t^m)$ is either 0 or close to $1 - 2\beta$ with distance bounded by $16k^2\varepsilon$.

Note that $f(\pi_t^m) = 0$ implies $\mu_x f_x(\pi_t^m) = 0$ for every x , hence $\phi(\cdot) = 0$ for all functions under consideration. On the other hand when $f(\pi_t^m) \neq 0$, then all

$\mu_x f_x(\pi_t^m)$ are nonzero except when $x_m = 1$. In this case these functions $\phi(\cdot)$ have the following Taylor expansions at corresponding points as follows,

$$\begin{aligned}\phi(\mu_0 f_0(\pi_t^m)) &= -\frac{1-k\beta}{2} + (\ln(1-k\beta))\mu_0 f_0(\pi_t^m) + \frac{(\mu_0 f_0(\pi_t^m))^2}{2(1-k\beta)} + O(\varepsilon^3), \\ \phi(\mu_j f_j(\pi_t^m)) &= -\frac{\beta}{2} + (\ln \beta)\mu_j f_j(\pi_t^m) + \frac{(\mu_j f_j(\pi_t^m))^2}{2\beta} + O(\varepsilon^3), \quad j \neq 0, j \neq m \\ \phi(f(\pi_t^m)) &= -\frac{1-\beta}{2} + (\ln(1-\beta))f(\pi_t^m) + \frac{f(\pi_t^m)^2}{2(1-\beta)} + O(\varepsilon^3), \\ \phi(f(\pi_t^m) - \mu_j f_j(\pi_t^m)) &= -\frac{1-2\beta}{2} + (\ln(1-2\beta))f(\pi_t^m) + \frac{f(\pi_t^m)^2}{2(1-2\beta)} - \\ &\quad (\ln(1-2\beta))\mu_j f_j(\pi_t^m) + \frac{(\mu_j f_j(\pi_t^m))^2}{2(1-2\beta)} - \frac{\mu_j f_j(\pi_t^m)f(\pi_t^m)}{1-2\beta} + O(\varepsilon^3), \quad j \neq 0, j \neq m.\end{aligned}$$

Recall Taylor's theorem with the remainder in Lagrange form says that the error term $O(\varepsilon^3)$ in the expansion of $\phi(\mu_0 f_0(\pi_t^m))$ equals $\frac{|\phi^{(3)}(\xi)|}{6}|\mu_0 f_0(\pi_t^m) - (1-k\beta)|^3$ for some ξ between $\mu_0 f_0(\pi_t^m)$ and $1-k\beta$. Since $|\mu_0 f_0(\pi_t^m) - (1-k\beta)| \leq 4k\varepsilon$, we have $|\xi - (1-k\beta)| \leq 4k\varepsilon$, hence $\xi \geq (1-k\beta) - 4k\varepsilon > 0$ if $\varepsilon < \frac{1-k\beta}{4k}$. Furthermore, we have $0 < \frac{1}{(1-k\beta)-4k\varepsilon} \leq \frac{2}{1-k\beta}$ as long as $\varepsilon \leq \frac{1-k\beta}{8k}$. Therefore,

$$\begin{aligned}\frac{|\phi^{(3)}(\xi)|}{6}|\mu_0 f_0(\pi_t^m) - (1-k\beta)|^3 &= \frac{1}{6\xi^2}|\mu_0 f_0(\pi_t^m) - (1-k\beta)|^3 \\ &\leq \frac{1}{6(1-k\beta-4k\varepsilon)^2}(4k\varepsilon)^3 \\ &\leq \frac{4}{6(1-k\beta)^2}(4k)^3\varepsilon^3 \leq \frac{k^{11}}{6(1-k\beta)^2}\varepsilon^3,\end{aligned}$$

when $0 < \varepsilon \leq \frac{1-k\beta}{k^7} < \frac{1-k\beta}{8k}$. Denote the constant in this upper bound by R_1 .

Similarly, let R_2, R_3 and R_4 denote the constants that we can get as upper bounds of the absolute values of error terms in the expansions of $\phi(\mu_j f_j(\pi_t^m))$, $\phi(f(\pi_t^m))$ and $\phi(f(\pi_t^m) - \mu_j f_j(\pi_t^m))$, respectively. We have

$$\begin{cases} R_1 \leq \frac{k^{11}}{6(1-k\beta)^2}, & \text{when } 0 < \varepsilon \leq \frac{1-k\beta}{k^7}; \\ R_2 \leq \frac{k^{14}}{6\beta^2}, & \text{when } 0 < \varepsilon \leq \frac{\beta}{k^7}; \\ R_3 \leq \frac{k^{20}}{6(1-\beta)^2}, & \text{when } 0 < \varepsilon \leq \frac{1-\beta}{k^7}; \\ R_4 \leq \frac{k^{20}}{6(1-2\beta)^2}, & \text{when } 0 < \varepsilon \leq \frac{1-2\beta}{k^7}. \end{cases} \quad (27)$$

Observe that $\mu_x^0 f_x^0$ and $\mu_x^1 f_x^1$ are both close to $\mu_x f_x$ with distance bounded by 3ε , hence the corresponding functions $\phi(\mu_x^0 f_x^0)$ and $\phi(\mu_x^1 f_x^1)$ have the same expansions as above, the same holds for functions $\phi(f^0)$, $\phi(f^1)$ and $\phi(f^0 - \mu_x^0 f_x^0)$, $\phi(f^1 - \mu_x^1 f_x^1)$.

We continue to use the Taylor expansions to expand the concavity conditions (15) and (16).

- Taylor expansion of external concavity condition (15).

When $f(\pi_t^m) \neq 0$, we have the following expansion,

$$\begin{aligned}
& \phi(f(\pi_t^m)) - \sum_x \phi(\mu_x f_x(\pi_t^m)) \\
&= \phi(f(\pi_t^m)) - \phi(\mu_0 f_0(\pi_t^m)) - \sum_{j=1, j \neq m}^k \phi(\mu_j f_j(\pi_t^m)) \\
&= (\ln(1 - \beta))f + \frac{1}{2(1 - \beta)}f^2 - (\ln(1 - k\beta))\mu_0 f_0 - \frac{1}{2(1 - k\beta)}(\mu_0 f_0)^2 \\
&\quad - \ln \beta \sum_{j=1, j \neq m}^k \mu_j f_j - \frac{1}{2\beta} \sum_{j=1, j \neq m}^k (\mu_j f_j)^2 + O(\varepsilon^3),
\end{aligned} \tag{28}$$

where constant in $O(\varepsilon^3)$ can be bounded by $R_1 + (k - 1)R_2 + R_3$ according to (27). Using Claim 6, we see that the first, third and fifth terms in (28) become 0 in (15). Let

$$F_m^{ext}(t) = \frac{1}{2(1 - \beta)}f^2 - \frac{1}{2(1 - k\beta)}(\mu_0 f_0)^2 - \frac{1}{2\beta} \sum_{j=1, j \neq m}^k (\mu_j f_j)^2.$$

Define $F_m^{ext,0}(t)$ and $F_m^{ext,1}(t)$ with f replaced by f^0 and f^1 , respectively, etc. Observe that $F_m^{ext}(t) = 0$ when $f(\pi_t^m) = 0$, hence in general $F_m^{ext}(t)$ is a correct representation of $\phi(f(\pi_t^m)) - \sum_x \phi(\mu_x f_x(\pi_t^m))$. Therefore, what we want to verify in (15) becomes

$$\int_{-\gamma_0}^{\gamma_1} \sum_{m=1}^k \left(F_m^{ext}(t) - \frac{F_m^{ext,0}(t) + F_m^{ext,1}(t)}{2} \right) dt + O(\varepsilon^4). \tag{29}$$

As $\gamma_0 + \gamma_1 \leq 4\varepsilon$, by (27), the constant in $O(\varepsilon^4)$ in (29) can be bounded by

$$8k(R_1 + (k - 1)R_2 + R_3) \leq 4k^{21} \left(\frac{1}{(1 - k\beta)^2} + \frac{1}{\beta^2} \right),$$

when $\varepsilon \leq \frac{1}{k^7} \min\{\beta, 1 - k\beta\}$.

- Taylor expansion of internal concavity condition (16).

A direct calculation gives,

$$\begin{aligned}
& \sum_{j=1}^k \sum_{b=0,1} \phi(f_{x_j=b}(\pi_t^m)) - k \sum_x \phi(\mu_x f_x(\pi_t^m)) \\
&= \phi(f(\pi_t^m)) - k\phi(\mu_0 f_0(\pi_t^m)) \\
&\quad + \sum_{j=1, j \neq m}^k \left(\phi(f(\pi_t^m) - \mu_j f_j(\pi_t^m)) - (k - 1)\phi(\mu_j f_j(\pi_t^m)) \right).
\end{aligned} \tag{30}$$

As did for the external case, when $f(\pi_t^m) \neq 0$ the above formula expands as follows,

$$\begin{aligned}
(30) &= (\ln(1 - \beta) + (k - 2) \ln(1 - 2\beta) - (k - 1) \ln \beta) f \\
&\quad + \left(\frac{1}{2(1 - \beta)} + \frac{k - 3}{2(1 - 2\beta)} \right) f^2 \\
&\quad + (\ln(1 - 2\beta) + (k - 1) \ln \beta - k \ln(1 - k\beta)) \mu_0 f_0 \\
&\quad - \frac{k}{2(1 - k\beta)} (\mu_0 f_0)^2 + \left(\frac{1}{2(1 - 2\beta)} - \frac{k - 1}{2\beta} \right) \sum_{j=1, j \neq m}^k (\mu_j f_j)^2 \\
&\quad + \frac{1}{1 - 2\beta} \mu_0 f_0 f + O(\varepsilon^3).
\end{aligned} \tag{31}$$

Claim 6 implies the first and third terms in (31) become 0 in (16). Let

$$\begin{aligned}
F_m(t) &= \left(\frac{1}{2(1 - \beta)} + \frac{k - 3}{2(1 - 2\beta)} \right) f^2 - \frac{k}{2(1 - k\beta)} (\mu_0 f_0)^2 \\
&\quad + \left(\frac{1}{2(1 - 2\beta)} - \frac{k - 1}{2\beta} \right) \sum_{j=1, j \neq m}^k (\mu_j f_j)^2 + \frac{1}{1 - 2\beta} \mu_0 f_0 f.
\end{aligned}$$

Define $F_m^0(t)$ and $F_m^1(t)$ similarly. Then $F_m(t)$ is a correct representation for (30). Therefore what we want to verify in (16) becomes

$$\int_{-\gamma_0}^{\gamma_1} \sum_{m=1}^k \left(F_m(t) - \frac{F_m^0(t) + F_m^1(t)}{2} \right) dt + O(\varepsilon^4). \tag{32}$$

Density functions in explicit form We continue to calculate functions explicitly that will be used for computing.

– In the protocol π_μ^\wedge .

Consider the interval $t \in [-\gamma_0, 0)$. Let $A = (s - 1)(t + \gamma_0) = (s - 1)t + (s - 1)\gamma_0$. The total active time $\Phi_0(t) = \Phi_j(t) = A$ for $s \leq j \leq k$, and $\Phi_j(t) = A - (t + \gamma_0)$ for $1 \leq j \leq s - 1$. Hence for $1 \leq m \leq s - 1$, we have,

$$\mu_j f_j(\pi_t^m) = \begin{cases} \mu_0 e^{-A}, & j = 0, \\ \mu_j e^{t + \gamma_0} e^{-A} = e^{\gamma_0} \beta e^t e^{-A}, & 1 \leq j \leq s - 1 \text{ and } j \neq m, \\ \mu_j e^{-A} = e^{\gamma_0} \beta e^t e^{-A}, & s \leq j \leq k, \\ 0, & j = m. \end{cases}$$

For $m \geq s$, we have $\mu_x f_x(\pi_t^m) = 0$ for all x . Therefore when $t \in [-\gamma_0, 0)$,

$$f(\pi_t^m) = \begin{cases} 0, & m \geq s, \\ (1 - (s - 1)\beta + (s - 2)e^{\gamma_0} \beta e^t) e^{-A}, & 1 \leq m \leq s - 1. \end{cases}$$

Similarly for the interval $t \in [0, \gamma_1)$, let $B = (s-1)(t + \gamma_0) + (k-s+1)t = kt + (s-1)\gamma_0$, the total active time is $\Phi_0(t) = B$, $\Phi_j(t) = B - (t + \gamma_0)$ for $1 \leq j \leq s-1$, and $\Phi_j(t) = B - t$ for $s \leq j \leq k$. Hence for all $1 \leq m \leq k$ we have,

$$\mu_j f_j(\pi_t^m) = \begin{cases} \mu_0 e^{-B}, & j = 0, \\ \mu_j e^{t+\gamma_0} e^{-B} = e^{\gamma_0} \beta e^t e^{-B}, & 1 \leq j \leq s-1 \text{ and } j \neq m, \\ \mu_j e^t e^{-B} = e^{\gamma_0} \beta e^t e^{-B}, & s \leq j \leq k \text{ and } j \neq m, \\ 0, & j = m. \end{cases}$$

Therefore when $t \in [0, \gamma_1)$,

$$f(\pi_t^m) = (1 - (s-1)\beta - (k-s+1)e^{\gamma_0}\beta + (k-1)e^{\gamma_0}\beta e^t)e^{-B}.$$

– In the protocol $\pi_{\mu^0}^\wedge$.

Using results from Section 6.1, we have,

$$\mu_x^0 f_x^0(\pi_t^m) = \begin{cases} (1 - \varepsilon\zeta)e^{-t} \mu_x f_x(\pi_t^m), & t \in [-\gamma_0, 0), x_s = 0, m \neq s, \\ (1 - \varepsilon\zeta) \mu_x f_x(\pi_t^m), & t \in [-\gamma_0, 0), x_s = 1, m \neq s, \\ (1 - \varepsilon\zeta) \mu_x f_x(\pi_t^m), & t \in [0, \gamma_1). \end{cases}$$

For the special case $m = s$ and $t \in [-\gamma_0, 0)$, we have,

$$\mu_j^0 f_j^0(\pi_t^s) = \begin{cases} (1 - \varepsilon\zeta) \mu_0 e^{-t} e^{-A}, & t \in [-\gamma_0, 0), j = 0, \\ (1 - \varepsilon\zeta) e^{\gamma_0} \beta e^{-A}, & t \in [-\gamma_0, 0), 1 \leq j \leq s-1, \\ 0, & t \in [-\gamma_0, 0), j = s, \\ (1 - \varepsilon\zeta) e^{\gamma_0} \beta e^{-t} e^{-A}, & t \in [-\gamma_0, 0), s+1 \leq j \leq k. \end{cases}$$

Therefore when $t \in [-\gamma_0, 0)$,

$$f^0(\pi_t^m) = \begin{cases} (1 - \varepsilon\zeta)((1 - e^{\gamma_0}\beta - (s-1)\beta)e^{-t} + (s-1)e^{\gamma_0}\beta)e^{-A}, & 1 \leq m \leq s, \\ 0, & s+1 \leq m \leq k. \end{cases}$$

When $t \in [0, \gamma_1)$, it is simply,

$$f^0(\pi_t^m) = (1 - \varepsilon\zeta)f(\pi_t^m).$$

– In the protocol $\pi_{\mu^1}^\wedge$.

Using results from Section 6.1, when $m = s$, then $\mu_x^1 f_x^1(\pi_t^m) = 0$ for all x for $t \in [-\gamma_0, \gamma_1]$. Therefore $f^1(\pi_t^s) = 0$ for all $t \in [-\gamma_0, \gamma_1]$.

When $m \neq s$, we have,

$$\mu_x^1 f_x^1(\pi_t^m) = \begin{cases} \mu_x^1 f_x(\pi_t^m), & t \in [-\gamma_0, 0), \\ (1 - \varepsilon e^{\gamma_0}\beta) e^t \mu_x f_x(\pi_t^m), & t \in [0, \gamma_1), x_s = 0, \\ (1 + \varepsilon\zeta) \mu_x f_x(\pi_t^m), & t \in [0, \gamma_1), x_s = 1. \end{cases}$$

Hence when $t \in [-\gamma_0, 0)$, we have $f^1(\pi_t^m) = (1 - \varepsilon e^{\gamma_0} \beta) f(\pi_t^m) + \varepsilon \mu_s f_s(\pi_t^m)$, and when $t \in [0, \gamma_1)$ we have $f^1(\pi_t^m) = (1 - \varepsilon e^{\gamma_0} \beta) e^t f(\pi_t^m) + (1 + \varepsilon \zeta - (1 - \varepsilon e^{\gamma_0} \beta) e^t) \mu_s f_s(\pi_t^m)$. Plug in f we get, when $t \in [-\gamma_0, 0)$,

$$f^1(\pi_t^m) = \begin{cases} 0, & m \geq s, \\ (1 + e^{\gamma_0} \beta (1 - \varepsilon e^{\gamma_0} \beta)) ((s-2)e^t - (s-1)e^{-\gamma_0}) e^{-A}, & 1 \leq m \leq s-1. \end{cases}$$

When $t \in [0, \gamma_1)$,

$$f^1(\pi_t^m) = \begin{cases} 0, & m = s, \\ (1 + e^{\gamma_0} \beta (1 - \varepsilon e^{\gamma_0} \beta)) ((k-2)e^t - (s-1)e^{-\gamma_0} - k + s) e^t e^{-B}, & m \neq s. \end{cases}$$

External information cost Using Wolfram Mathematica with results from Section 6.4 and 6.4, we obtain

$$(29) = \frac{(k+5s-6)(1-2\beta)\beta}{12(1-\beta)\ln 2} \varepsilon^3 + O(\varepsilon^4). \quad (33)$$

Therefore, using the bound of the error term given in Section 6.4, one finds (33) > 0 as long as

$$\varepsilon < \min \left\{ \frac{(k+5s-6)(1-2\beta)\beta}{12(1-\beta)\ln 2} \Big/ 4k^{21} \left(\frac{1}{(1-k\beta)^2} + \frac{1}{\beta^2} \right), \frac{1}{k^7} \min\{\beta, 1-k\beta\} \right\}.$$

Note that $\frac{2}{1/x+1/y} = \frac{2xy}{x+y} \geq \min\{x, y\}$ for all $x, y > 0$. Simplifying the above formula, one obtains (33) > 0 as long as

$$\varepsilon < ck^{-20} \min\{\beta, 1-k\beta\}^3,$$

for some constant $c > 0$. So we have verified the concavity condition (15) is satisfied for all ε -weak signals such that ε is no greater than $ck^{-20} \min\{\beta, 1-k\beta\}^3$.

Let μ^E denote the distribution in Claim 1, we have $|\mu - \mu^E| \leq 1 - k\beta$. Let μ' be defined as $\mu'_{s-1} = 0$, $\mu'_s = e^{\gamma_0} \beta + \beta$, and $\mu'_j = \mu_j$ for all other j , then $|\mu - \mu'| = \beta$. Observe that μ' is external trivial, hence $\mu^E, \mu' \in \Omega$ (the Ω we chose at the beginning of Section 6.2). Therefore we have $\delta(\mu) \leq \min\{\beta, 1-k\beta\}$. Thus as we choose $w(x) = ck^{-20}x^4$, the concavity condition (15) is satisfied for all $w(\delta(\mu))$ -weak signals because

$$w(\delta(\mu)) \leq ck^{-20} \min\{\beta, 1-k\beta\}^4 < ck^{-20} \min\{\beta, 1-k\beta\}^3.$$

By Theorem 5, we have proved the protocol π^\wedge in Figure 1 is optimal for external information cost.

Internal information cost Similarly, using Wolfram Mathematica, we obtain

$$(32) = \begin{cases} \frac{(k+5s-6)(1-2\beta)\beta}{12(1-\beta)\ln 2}\varepsilon^3 + O(\varepsilon^4), & k = 2, \\ \frac{(k+5s-6)((3k-2)\beta^2-4(k-1)\beta+k-1)\beta}{12(1-\beta)(1-2\beta)\ln 2}\varepsilon^3 + O(\varepsilon^4), & k \geq 3. \end{cases} \quad (34)$$

As did in Section 6.4, one can show (34) is positive when ε is sufficiently small. And furthermore one can pick an appropriate function w to verify that the concavity condition (16) is satisfied for all $w(\delta(\mu))$ -weak signals. Hence by Theorem 5, our protocol is optimal for internal information cost.

References

- [BBCR10] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao, *How to compress interactive communication [extended abstract]*, STOC'10, ACM, New York, 2010, pp. 67–76.
- [BGPW13] Mark Braverman, Ankit Garg, Denis Pankratov, and Omri Weinstein, *From information to exact communication (extended abstract)*, STOC'13, ACM, New York, 2013, pp. 151–160.
- [BGPW16] ———, *Information lower bounds via self-reducibility*, Theory of Computing Systems **59** (2016), no. 2, 377–396.
- [BR14] Mark Braverman and Anup Rao, *Information equals amortized communication*, IEEE Trans. Inform. Theory **60** (2014), no. 10, 6058–6069.
- [Bra15] Mark Braverman, *Interactive information complexity*, SIAM Journal on Computing **44** (2015), no. 6, 1698–1739.
- [BS15] Mark Braverman and Jon Schneider, *Information complexity is computable*, arXiv preprint arXiv:1502.02971 (2015).
- [CT12] Thomas M Cover and Joy A Thomas, *Elements of information theory*, John Wiley & Sons, 2012.
- [DF16] Yuval Dagan and Yuval Filmus, *Grid protocols*, In preparation, 2016.
- [DFHL16] Yuval Dagan, Yuval Filmus, Hamed Hatami, and Yaqiao Li, *Trading information complexity for error*, arXiv preprint arXiv:1611.06650 (2016).
- [Gro09] Andre Gronemeier, *Asymptotically optimal lower bounds on the nih-multi-party information*, arXiv preprint arXiv:0902.1609 (2009).
- [MI11] Nan Ma and Prakash Ishwar, *Some results on distributed source coding for interactive function computation*, IEEE Trans. Inform. Theory **57** (2011), no. 9, 6180–6195.
- [MI13] ———, *The infinite-message limit of two-terminal interactive source coding*, IEEE Trans. Inform. Theory **59** (2013), no. 7, 4071–4094.
- [Raz92] A. A. Razborov, *On the distributional complexity of disjointness*, Theoret. Comput. Sci. **106** (1992), no. 2, 385–390.
- [Yao79] Andrew Chi-Chih Yao, *Some complexity questions related to distributive computing (preliminary report)*, STOC '79, ACM, 1979, pp. 209–213.